ANÁLISIS Y EVALUACIÓN DE RIESGOS INFORMÁTICOS EN SERVIDORES DE PROYECTOS ADMINISTRATIVOS DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR

JEFERSON CORTES POVEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2020

ANÁLISIS Y EVALUACIÓN DE RIESGOS INFORMÁTICOS EN SERVIDORES DE PROYECTOS ADMINISTRATIVOS DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR

JEFERSON CORTES POVEDA

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Asesor: JULIO ALBERTO VARGAS FERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

Nota de aceptación

_____

_____

_____

_____
Firma presidente de jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, D.C., Abril de 2020

DEDICATORIA

A Dios, a mi esposa, a mi hermano y a mi familia los cuales se encuentran en cada una de las etapas planeadas, llenándome de fuerza y esperanza para lograr los objetivos propuestos.

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Julio Alberto Vargas, asesor del proyecto

A la Universidad Nacional Abierta y a Distancia UNAD

A todas aquellas personas que de una u otra forma colaboraron en la elaboración de este proyecto.

Bogotá, D.C., Abril de 2020

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

pág.

RESUMEN

Los ataques informáticos se están convirtiendo en un reto y un punto muy importante a revisar profundamente en las grandes empresas ya que las pérdidas que se han generado a partir de estos son muy grandes. Así mismo, las instituciones de educación superior deben tener en cuenta este aspecto en sus modelos tecnológicos, tanto de infraestructura como aplicaciones y sistemas de información, debido al gran volumen de información de usuarios que manejan constantemente.

El presente trabajo de grado tiene como objetivo revisar las condiciones de seguridad informática de los servidores de una institución de educación superior, revisión que comprende la evaluación de riesgos desde lo físico hasta lo más intangible como lo son aplicaciones y sistemas de información.

Para la revisión de la seguridad informática de los servidores se utiliza la metodología Magerit la cual comienza con la descripción de los activos de la empresa, que en este caso se limita a los servidores y los sistemas de información que gestionan la información de los usuarios.

Una vez identificados los activos, se detectaron las amenazas que puede afectarlos, se plantea la probabilidad de ocurrencia de estas amenazas sobre los activos y se mide el impacto de los riesgos sobre los activos. A continuación, se determinan los posibles controles que se sugieren aplicar a los riesgos identificados, controles que reducen el impacto y la degradación de los activos y al mismo tiempo aumentan los niveles de seguridad de la información de la institución.

Esta evaluación se apoya con la herramienta EAR/PILAR la cual incorpora toda la metodología Magerit y cada una de sus fases, partiendo de la gestión de los activos para posteriormente llegar a la identificación los riesgos y la proposición de los controles.

Con la metodología Magerit y la herramienta EAR/PILAR se logró mostrar y evidenciar los niveles de riesgo antes y después de aplicar los controles propuestos y se pudo contrastar el riesgo e impacto potencial y el riesgo e impacto residual que se hallaron en la revisión.

ABSTRACT

Computer attacks are becoming a challenge and a very important point to review deeply in large companies since the losses that have been generated from these are very large. Likewise, higher education institutions must take this aspect into account in their technological models, both of infrastructure and applications and information systems, due to the large volume of information from users that they constantly handle.

The purpose of this work is to review the computer security conditions of the servers of a higher education institution, a review that includes the assessment of risks from the physical to the most intangible, such as applications and information systems.

The Magerit methodology is used to review the computer security of the servers, which begins with the description of the company's assets, which in this case is limited to the servers and information systems that manage user information.

Once the assets have been identified, the threats that may affect them are detected, the probability of occurrence of these threats on the assets is considered, and the impact of the risks on the assets is measured. Thus, the possible controls that are suggested to be applied to the identified risks are determined; controls that can reduce the impact and degradation of assets and at the same time increase the security levels of the institution's information.

This evaluation is supported by the EAR / PILAR tool which incorporates all the Magerit methodology and each of its phases, based on the management of the assets to subsequently identify risks and propose controls..

With the Magerit methodology and the EAR / PILAR tool, it was possible to show and demonstrate the risk levels before and after applying the proposed controls and it was possible to contrast the risk and potential impact and the risk and residual impact found in the review.

INTRODUCCIÓN

El presente trabajo aplicado está orientado a la revisión de la seguridad informática de ciertos activos en una institución de educación superior, revisión que comprende la evaluación de riesgos desde lo físico hasta lo más intangible como lo son aplicaciones y sistemas de información.

Según un estudio realizado en Latinoamérica, Colombia se encuentra en una calificación media frente al tema de la seguridad informática. Con una evaluación realizada a 6 países, Colombia quedó en el puesto número 5, siendo el primero el peor de los 6. Esto se debe a que ha mejorado el estándar en las empresas frente a la gestión de la seguridad de la información[1].

Sin embargo, Colombia, dentro de sus políticas para la creación de pymes y corporaciones, debería exigir ciertas condiciones de seguridad informática y garantizar la implementación de SGSI, apoyando estas iniciativas con fondos del estado para las pymes y corporaciones que se encuentran en su fase de crecimiento empresarial.

Así pues, el trabajo aplicado se enfoca en realizar una evaluación de los riesgos a los que se someten los activos de una institución de educación superior para revisar qué controles pueden aplicarse frente a las amenazas y vulnerabilidades que pueden afectar la información de esta institución.

Esta evaluación se fundamentó en la metodología Magerit, metodología que comienza desde la identificación de los activos de la institución hasta todos los procesos para controlar, eliminar, compartir y aceptar el riesgo.

De esta evaluación se presentaron todos los vectores de ataques a los que se encuentran expuestos los servidores y se produjeron estrategias para el tratamiento de riesgos basándose continuamente en la metodología Magerit.

Paralelamente se generaron salvaguardas de seguridad para la revisión periódica de los servidores, salvaguardas que colaboran con la mitigación y el tratamiento de los riesgos encontrados.

Finalmente se entrega a la institución una guía de recomendaciones donde se describe los riesgos encontrados, el impacto de estos riesgos, las estrategias de tratamiento formuladas, recomendando aplicar ésta guía para evitar incidencias a futuro con los servidores y los proyectos de la institución.

[1] COMPARITECH. Which countries have the worst (and best) cybersecurity?. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: website: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

TÍTULO

ANÁLISIS Y EVALUACIÓN DE RIESGOS INFORMÁTICOS EN SERVIDORES DE PROYECTOS ADMINISTRATIVOS DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR

1. PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

La sistematización de los procesos empresariales ha permitido que las instituciones de educación superior crezcan y mejoren la accesibilidad de los servicios a toda la población, llegando a zonas de difícil ingreso.

Esta sistematización a su vez causa una centralización y masificación de información de todas las personas que inician su vida académica, dando como resultado para las instituciones de educación superior la apropiación de nuevos retos, entre ellos, la protección de la información.

La información que se obtiene es almacenada en servidores los cuales están encargados no solo de guardar la información, sino también de ejecutar todos los sistemas de información que se encargan de convertir esta información en cifras y estadísticas para las instituciones de educación superior.

Otro propósito fundamental de los servidores es la ejecución de los sistemas de información financieros de la institución, sistemas de información que permiten la administración de presupuestos, planeación y vida financiera de todos los clientes, en el caso de las Instituciones de Educación Superior, estudiantes universitarios.

Así pues, los servidores en su esencia básica se convierten en piezas importantes de un gran flujo de información que va desde la creación y matriculación de los usuarios hasta la gestión académica, financiera y admirativa de cada uno.

Una vez mostrada la importancia de los servidores en una institución de educación superior la problemática que resuelve este trabajo aplicado es la revisión y evaluación de los riesgos informáticos a los que se encuentran expuestos los servidores de una institución de educación superior con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información.

1.2 JUSTIFICACIÓN

El presente trabajo aplicado se enfocará a revisar y verificar los riesgos a los que se encuentran expuestos los servidores donde se almacena información privada empresarial y se ejecutan proyectos con enfoques administrativos y académicos de una institución de educación superior.

La exigencia principal por la cual se realiza el presente trabajo de grado es por la necesidad que tienen las instituciones de educación superior de proteger la información de sus estudiantes, profesores y administrativos. Cabe aclarar que por tratarse de instituciones del sector educativo, la información que se almacena pueden contener datos personales de los estudiantes los cuales en algunos casos son menores de edad.

Así mismo, a nivel empresarial, la institución debe garantizar que sus servidores cumplan con los estándares de seguridad adecuados para asegurar que la información y los procesos no tengan intervención de terceros.

Este trabajo se convierte en el fundamento y el inicio de una revisión de seguridad informática total que se puede llevar a cabo en un futuro en la institución dando paso a la inclusión de todos los componentes como los elementos de la infraestructura de las redes de comunicaciones, espacios de trabajo, computadores clientes, etc.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Evidenciar los riesgos a los que se encuentran expuestos los servidores de proyectos de una institución de educación superior, con el fin de generar recomendaciones de seguridad que garanticen la disponibilidad, confidencialidad e integridad de la información.

2.2 OBJETIVOS ESPECÍFICOS

- Evidenciar el estado actual y el estado esperado de los servidores frente a los niveles de riesgos y el nivel de impactos.

- Identificar los vectores de ataque a los cuales están expuestos los proyectos de la institución.

- Generar estrategias para el tratamiento de riesgos informáticos encontrados en los servidores.

- Desarrollo de guía de buenas prácticas para garantizar la seguridad de los servidores de los proyectos.

3. MARCO REFERENCIAL

3.1 MARCO CONCEPTUAL

Servidores. Los servidores son todos aquellos dispositivos que se encargan de guardar toda la información de las organizaciones, además de ejecutar todas las aplicaciones para el correcto funcionamiento de los sistemas de información de la empresa. Los servidores poseen recursos que dependiendo la finalidad pueden ser utilizados por los diferentes sistemas de información para hacer transacciones de datos como consultas, creación y actualización dependiendo el caso.[2]

Proyectos TI. Un proyecto de tecnología se define como todos aquellos productos o servicios que a partir de la tecnología brindan un beneficio a una empresa u organización, solucionando problemas e incidentes a partir de innovaciones tecnológicas a partir de la implementación de software.[3]

Seguridad de la Información. La seguridad de la información se define como la protección de los datos almacenados evitando que dañen las características de éstos.[4]

Una definición puntual de la norma ISO/IEC 17799 es: "La norma ISO/IEC 17799 define la Seguridad de la Información como la preservación de su confidencialidad, su integridad y su disponibilidad *(medidas conocidas por su acrónimo "CIA" en inglés: Confidentiality, Integrity, Availability)".*[5]

Seguridad Informática. La seguridad informática tiene varias definiciones de las cuales se resaltan algunas:

- Se define la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan con llevar daños sobre la información, comprometer su

[2] LUJÁN MORA, S. Programación de aplicaciones web: historia, principios básicos y clientes web. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://rua.ua.es/dspace/handle/10045/16995

[3] RUIZ PALMERO, J., & SÁNCHEZ RODRÍGUEZ, J. El impacto del proyecto de centros TIC desde la experiencia vivida por el alumnado. 2007. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: https://idus.us.es/xmlui/handle/11441/45643.

[4] MAIWALD, E., & MIGUEL, E. A. Fundamentos de seguridad de redes. México: McGraw-Hill, 2005.

[5] DÍAZ, F. J., HARARI, V., & VENOSA, P. Auditoría de seguridad de organizaciones, fortalezas y debilidades de la norma ISO 17799. Presentado en V Workshop de Investigadores en Ciencias de la Computación. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://hdl.handle. net/109 15/21394

confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.[6]

- “La protección contra todos los daños sufridos o causados por la herramienta informática y originados por el acto voluntario y de mala fe de un individuo.”[7]
Desde un punto de vista objetivo se puede definir como todas las medidas que toman las organizaciones o empresas para evitar que los procesos administrativos tengan alguna dificultad al respecto, por el daño, eliminación o filtración de información.

Riesgo Informático. Un riesgo informático se puede describir como las debilidades que tiene un sistema de información, las cuales deben ser detectadas para su control, ya que estas pueden producir un daño en la información o en los procesos. [8]

Hoy en día, los sistemas de calidad de la empresa, son los encargados de la descripción de los procesos y su mejora, lo que incluye, la evaluación de riesgos de cada uno. Los sistemas de calidad se convierten en detectores de riesgos, lo que permite recoger información de éstos y poseer control de los mismos.[9]

Un riesgo informático, puede crear un impacto fuerte o leve, dependiendo donde se ubica y si se puede detectar a tiempo. Por ejemplo, la desactivación del Firewall de un Sistema por una situación especial, abre la posibilidad de intrusión de entes exteriores, lo que puede causar un daño enorme por la pérdida o filtración de información.[10]

Incidente de Seguridad. Previamente, se realizó la descripción de los riesgos informáticos, como la posibilidad de que suceda algún daño o suceso inesperado. Un incidente de seguridad es la ejecución de algún procedimiento inesperado, donde hubo una pérdida o filtración de información o donde hubo un daño al sistema, entre otros. [11]

---

[6] GALINDO, G., & MAURICIO, D. Desarrollo del sistema de gestión de seguridad de la información (sgsi) alineado con el estándar iso 27001 y sus requisitos básicos en la aplicación del ciclo phva. 11. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: https://idus.us.es/xmlui/handle/11441/45643.

[7] ROYER. 2004. Estudio comparativo entre las metodologías cramm y magerit para la gestión de riesgo de ti en las mpymes. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: revistas.uazuay.edu.ec>index.php › udaakadem › article › download

[8] RAYA CABRERA & RAYA GONZALEZ. Riesgo Informático. Bogotá: Grupo Editorial Norma, 2014. 356 p.

[9] Ibíd., p. 13

[10] Ibíd., p. 14

[11] GOMEZ LOPEZ & GÒMEZ LÓPEZ. Seguridad informática. 2014. Bogotá: Editorial Rama. 108 p.

Un incidente de seguridad es un suceso que puede detener los procesos de la empresa y si no se tiene una gestión oportuna puede ocasionar perdidas que pueden llevar al quiebre de la empresa.[12]

Vulnerabilidad. Se define como vulnerabilidad, las posibles entradas, fallas, mal funcionamiento o malas configuraciones realizadas, que presenten un sistema de seguridad, las cuales pueda aprovechar individuos como hackers, para alterar la información. [13]

Riesgo Residual. El riesgo residual puede definirse como el riesgo remanente luego de la aplicación de medidas a riesgos encontrados destinados a mitigar dichos riesgos. [14]

Activos. Elementos que representan valor para la organización. Pueden definirse como todos los recursos de hardware, software y documentación privada que tienen las empresas. [15]

Amenazas. Se define como vulnerabilidad, las posibles entradas, fallas, mal funcionamiento o malas configuraciones realizadas, que presenten un sistema de seguridad, las cuales pueda aprovechar individuos como hackers, para alterar la información. [16]

Impacto Potencial. El impacto es la medida de daño a raíz de la materialización de una amenaza. El impacto potencial es el impacto que pueden tener los activos cuando se genera la aplicación de los controles sobre los riesgos encontrados. [17]

---

[12] Ibíd., p. 25

[13] SOLARTE, F. N. S., ROSERO, E. R. E., & BENAVIDES, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5). [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

[14] SENA, Leonardo; TENZER, Simón Mario. (2014). Introducción al riesgo Informático. Cátedra Introducción a la Computación. Montevideo: Universidad de la República, Facultad de Ciencias Económicas y de Administración. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://www.academia.edu/14745302/Estructura_del_documento_de_riesgos_inform%C3%A1ticos

[15] CHANGO, Christian Damian Torres. CHICAIZA, Denis (2019). Plan de Seguridad Informática aplicando ISO 27001 para proteger la información y activos en una entidad privada. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://redi.uta.edu.ec/jspui/handle/123456789/73770

[16] SOLARTE, F. N. S., ROSERO, E. R. E., & BENAVIDES, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5). [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

[17] GARCÍA HERNÁNDEZ, David Alejandro. (2017). Análisis y gestión de riesgos en el marco del SGSI, basado en la Metodología MAGERIT y apoyado en un API Web para su ejecución. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://repository.udistrital.edu.co/handle/11349/15616

Impacto Residual. El impacto es la medida de daño a raíz de la materialización de una amenaza. El impacto residual es el impacto remanente luego de la aplicación de los controles sobre los riesgos encontrados. [18]

Controles. Son los procedimientos efectuados para lograr asegurar el cumplimiento de los objetivos definidos cuando se hace una revisión de riesgos. Estos procedimientos permiten mitigar los riesgos encontrados. [19]

3.2 MARCO TEÓRICO

3.2.1 Amenazas y ataques a servidores. Una amenaza lógica es software o código que de una forma u otra pueden afectar o dañar a nuestro sistema, creados de forma intencionada para ello, software malicioso, también conocido como malware. Entre otros encontramos:

- Herramientas de seguridad: Existen herramientas para detectar y solucionar fallos en los sistemas, pero se pueden utilizar para detectar esos mismos fallos y aprovecharlos para atacarlos.[20]
- Rogueware o falsos programas de seguridad: También denominados Rogue, FakeAVs, Badware, Scareware, son falsos antivirus o anti espías.[21]
- Puertas traseras o backdoors: Los programadores insertan “atajos” de acceso o administración, en ocasiones con poco nivel de seguridad. [22]
- Virus: Secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace. Detrás de la palabra virus existe todo un conjunto de términos, dentro de lo que se conoce como malware.[23]

- Gusano o Worm: Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, normalmente mediante correo electrónico basura o spam.[24]

- Troyanos o Caballos de Troya: Aplicaciones con instrucciones escondidas de forma que éste parezca realizar las tareas que un usuario espera de él, pero que

---

[18] GARCÍA HERNÁNDEZ, David Alejandro. (2017). Análisis y gestión de riesgos en el marco del SGSI, basado en la Metodología MAGERIT y apoyado en un API Web para su ejecución. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://repository.udistrital.edu.co/handle/11349/15616

[19] SENA, Leonardo; TENZER, Simón Mario. (2014). Introducción al riesgo Informático. Cátedra Introducción a la Computación. Montevideo: Universidad de la República, Facultad de Ciencias Económicas y de Administración. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://www.academia.edu/14745302/Estructura_del_documento_de_riesgos_inform%C3%A1ticos

[20] COSTAS SANTOS, J. Seguridad y alta disponibilidad. 2014 [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://site.ebrary.com/lib/unadsp/docDetail.action?docID=11046042

[21] Ibíd., p. 23

[22] Ibíd., p. 24

[23] Ibíd., p. 25

[24] Ibíd., p. 26

realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario. [25]

- Programas conejo o bacterias: Programas que no hacen nada útil, simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio.[26]

- Canales cubiertos: Canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; un proceso transmite información a otros que no están autorizados a leer dicha información.[27]

Las principales amenazas realizadas manualmente por atacantes a las que se enfrenta una red son las siguientes:

- Recopilación de información (harvesting): El intruso busca obtener información acerca de la topología de red, tipos de dispositivos presentes y su configuración. Gracias a esta información puede descubrir vulnerabilidades y puntos de entrada.[28]

- Intercepción de tráfico (sniffing): El intruso intercepta el tráfico de forma pasiva, es decir, no lo modifica, en busca de contraseñas e información sensible que circula por la red.

- Falsificación (spoofing): El intruso oculta su identidad real, haciéndose pasar por otro usuario o equipo. Suele utilizarse para enmascarar la dirección real de procedencia de un ataque o para burlar un sistema de control de acceso en función de la dirección IP de origen. Es considerado un ataque por spoofing tanto la modificación de paquetes existentes en la red como la creación de nuevos cuyo objeto es falsear la identidad de algún componente de la transmisión de un mensaje. [29]

- Secuestro de sesión (hijacking): El intruso utiliza una aplicación para simular el comportamiento del cliente o del servidor, o bien intercepta los paquetes de información por la red pudiendo visionarlos y modificarlos a su antojo. Como consecuencia, el servidor o el cliente creen estar comunicándose con el equipo legítimo, cuando en realidad se trata del equipo del atacante, que aparece a

[25] Ibíd., p. 27
[26] Ibíd., p. 28
[27] COSTAS SANTOS, J. Op. Cit. p. 15
[28] ÁLVAREZ MARAÑÓN, G., & PÉREZ GARCÍA, P. P. (2004). Seguridad informática para empresas y particulares. 2004. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://site.ebrary.com/lib/unadsp/docDetail.action?docID=10498593
[29] Ibíd., p. 30

todos los efectos como el destino auténtico. Se utiliza típicamente para obtener información de autenticación y datos sensibles. A este tipo de ataques también se les conoce como ataques de hombre en el medio (Man-In-The-Middle o MITM).[30]

- Denegación de servicio (DoS): El intruso busca denegar a los usuarios legítimos el acceso a los servidores o servicios de la red, inundándola con tráfico espurio que consuma todo su ancho de banda y recursos. Cabe destacar un gran grupo dentro de este tipo de ataques conocido bajo el nombre de denegación de servicio distribuida (Distributed Denial of Service o DDoS) en el cual se coordinan varios sistemas para realizar un ataque simultáneo contra un objetivo definido.[31]

3.2.2 Amenazas y ataques WEB. Las organizaciones que hacen uso de las TICs aún desconocen sobre las consecuencias de las vulnerabilidades de seguridad en aplicaciones web más importantes. A continuación se presentan los ataques principales, de muchos:

- Inyección: Las fallas de inyección, tales como SQL, OS, LDAP, ocurren cuando datos no confidenciales son enviados a un intérprete como parte de un comando o consulta, tratando de engañar al intérprete en ejecutar comandos no intencionados o acceder datos no autorizados.[32]

- Secuencia de Comandos en Sitios Cruzados: Las fallas XSS ocurren cada vez que una aplicación toma datos no confidenciales y los envía al navegador web sin una validación y codificación apropiada. XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso. [33]
- Configuración de Seguridad Incorrecta: Una buena seguridad requiere tener definidas e implementada una configuración segura para la aplicación, marcos de trabajo, servidores de aplicación, servidores web, base de datos, y plataformas. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto.

- Exposición de datos sensibles: Muchas aplicaciones web no protegen adecuadamente datos sensibles tales como números de tarjetas de crédito, o credenciales de autenticación. Los datos sensibles requieren de métodos de

[30] Ibíd., p. 31
[31] Ibíd., p. 35
[32] SAUCEDO, A. L. H., & MIRANDA, J. M. (2016). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web. 4(1). 2016 [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://revistas cientificas.udg.mx/index.php/REC/article/view/5208
[33] Ibíd., p. 40

protección adicionales tales como el cifrado de datos, así como también de precauciones especiales en un intercambio de datos con el navegador. [34]

- Falsificación de Petición en Sitios Cruzados (CSRF): Un ataque CSRF obliga al navegador de una víctima autenticada a enviar una petición HTTP falsificado, incluyendo la sesión del usuario y cualquier otra información de autenticación incluida automáticamente, a una aplicación web vulnerable.[35]

3.2.3 Tipos de auditoria. Los servicios de auditoría pueden ser aplicarse a diferentes elementos:

- Auditoría de seguridad interna. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.[36]

- Auditoría de seguridad perimetral. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.

- Test de intrusión. El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.[37]

- Análisis forense. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis postmortem.

- Auditoría de páginas web. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc. [38]

Auditoría de código de aplicaciones. Análisis del código tanto de aplicaciones de páginas web como de cualquier tipo de aplicación, independientemente del lenguaje empleado.

---

[34] Ibíd., p. 45
[35] Ibíd., p. 43
[36] ESCRIVÁ GASCÓ, G., ROMERO SERRANO, R. M., & RAMADA, D. J. Seguridad informática. 2013. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://site.ebrary.com/lib/unadsp/docDetail.action?docID=10820963
[37] Ibíd., p. 52
[38] Ibíd., p. 53

3.3 MARCO METODOLÓGICO

3.3.1 Magerit. Es una metodología de análisis y gestión de riesgos elaborada por el *Consejo Superior de Administración Electrónica de España*, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar

Las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

Puntualmente Magerit se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas. [39]

3.3.2 Objetivos de Magerit. Magerit persigue los siguientes Objetivos Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso. [40]

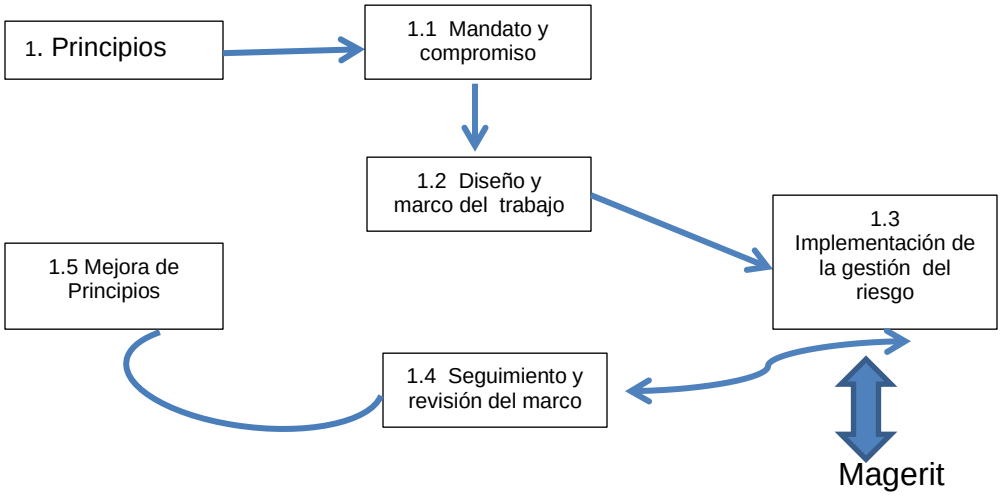
Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones

[39] MAGERIT, Pilar. Metodología práctica para gestionar riesgos. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: WeLiveSecurity website: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

[40] Magerit, Pilar. Metodología de análisis y gestión de riesgos de los sistemas de información. V. 3 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https:// administracióneléctronica. gob.es> pae.home>

teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Figura 1. Metodología Magerit



Fuente: autor

EAR/PILAR. Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit.

Los activos están expuestos a amenazas que, cuando se materializan, degradan el activo, produciendo un impacto. Si se estima la frecuencia con que se materializan las amenazas, podemos deducir el riesgo al que está expuesto el sistema. Degradación y frecuencia califican la vulnerabilidad del sistema.

El gestor del sistema de información dispone de salvaguardas, que o bien reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto. Dependiendo del grado de implantación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo que se denomina riesgo residual.[41]

[41] MAGERIT, Pilar. Herramientas para el análisis de riesgos. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https:// www.ccn-cert.cni.es › soluciones-seguridad › ear-pilar

3.4 MARCO HISTÓRICO

- En agosto de 2016 se muestra que el 43% de las empresas colombianas no están preparadas contra los ciberataques. [42]

- En octubre de 2016 se publica un artículo donde se describe la realización de un pentesting utilizando la metodología XP. En este artículo se plasman todas las pruebas que se pueden realizar y las herramientas utilizadas para ello.

Las pruebas a realizar son:

- Recolección de información
- Revisión de la configuración
  - Pruebas de autenticación
  - Pruebas de autorización
  - Pruebas de lógica de negocio
  - Pruebas de validación de datos
  - Pruebas de servicios web
  - Pruebas Ajax
  - Pruebas de denegación de servicio[43]

- En mayo de 2017 una de las empresas de telecomunicaciones más grande del mundo sufre un ataque por el virus Ransomware. La empresa tuvo que apagar sus equipos mientras resolvieron el incidente.[44]

- En abril de 2017 se genera un pentesting de un aplicativo web desarrollado en PHP 5, donde se hace referencia a todo el sistema legal colombiano respecto a los ataques web. Se configura un ambiente de pruebas y se procede a montar una plataforma en PHP, realizando las pruebas pertinentes.[45]

- En julio de 2017 se genera un estudio donde se verifica si la herramienta OWASP-ZAP puede generar controles para contrarrestar ataques por inyección SQL en plataformas creadas con frameworks para PHP.

---

[42] REVISTA DINERO. (2018). Colombia tuvo pérdidas de un billón por ciberataques. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://www.dinero.com/pais/articulo/colombia-tuvo-perdidas-de-1-billon-por-ciberataques/224404

[43] PONCE, S., & PATRICIO, E. (2018). Análisis de los ataques a aplicaciones web SQL Injection y Cross Site Scripting y sus medidas de precaución y defensa. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://repositorio.utn.edu.ec/handle/123456789/7803

[44] EL MUNDO. Hackean la red interna de Telefónica y de otras grandes empresas españolas. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html

[45] PINZÓN, G., & ALFONSO, H. Pentesting al proyecto web «Quadodo Login Script» desarrollado y soportado en lenguaje PHP versión 5.5.0. 2017. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://repository.unad.edu.co/handle/10596/13378

En este estudio se hace una aplicación con el framework Codelgneiter y luego bajo la aplicación OWASP se analizan todos los riesgos de ésta.[46]

- En septiembre de 2017 se registran un total de 542.465 ataques informáticos en Colombia.[47] En total han presentado un total de 198 millones de ataques, según lo revela un informe de la firma de ciberseguridad Digiware.

- En diciembre de 2017 se publica un artículo donde se describe como generar un buen hacking ético y las herramientas para hacerlo. Se hace un barrido sobre los principales ataques a sitios web, los tipos de pruebas de penetración y las etapas esenciales para generar un pentesting.[48]

- En diciembre de 2018 se detecta que Colombia ha sido uno de los países con más ataques cibernéticos donde 2 de cada 3 organizaciones consultadas revelaron que fueron víctimas de ciberataques.[49]

- En octubre de 2019 se revela que los reportes superan más de 28.000 casos de ciberataques en Colombia. Los incidentes cibernéticos en el país tuvieron un incremento del 54 % con respecto al 2018.[50]

3.5 MARCO LEGAL

Las leyes que han formado todo el contexto legal frente a la seguridad informática en Colombia, vienen formándose desde el año 1988. A continuación se hará un recorrido histórico revisando año a año la constitución actual de la seguridad informática:

1988. Ley de Protección de datos de 1988.[51]

---

[46] JIMÉNEZ, L. de, & Elizabeth, R. (2017). Pruebas de penetración en aplicaciones web usando hackeo ético. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://www.redicces.org.sv:80/jspui/handle/10972/3018

[47] Periodico El Tiempo, R. (2017). Informe sobre ataques informáticos en Colombia. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

[48] BASTIDAS, E., & Guillermo, C. (2017). Identificación de vulnerabilidades de los servicios tecnológicos de la unión de cooperativas de ahorro y crédito del norte aplicando la práctica de Pentesting. . [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://repositorio.utn.edu.ec/handle/ 1234567 89/7396

[49] Periodico La Republica. (2018). Informe sobre ataques informáticos en Colombia. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

[50] EL TIEMPO. (2019). En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

1989. Decreto 1360, de 23 de junio de 1989, por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor.[52]

1990. Decreto 1900 de 19 de agosto de 1990, por el cual se reforman las normas y estatutos que regulan las actividades y servicios de telecomunicaciones y afines.[53] .

1995. Decreto 2150 de 1995 sobre sistemas electrónicos, de 5 de diciembre de 1995, que busca la simplificación de trámites ante Entidades Estatales. (Diario Oficial 42.137, del 6 de diciembre de 1995).[54] .

1998. Proyecto de Ley 227 de 21 de abril de 1998, por medio del cual se define y Reglamenta el Acceso y el uso del Comercio Electrónico.

1999. Decreto 1487/ 1999, de 12 de Agosto, por Medio del Cual se Autoriza el Sistema Declaración y Pago Electrónico de la DIAN y se Establecen algunos Parámetros Operativos para la Presentación de las Declaraciones Tributarias y el Pago de los Impuestos por Vía Electrónica.

Ley 527 de 18 de agosto de 1999, sobre Mensajes de Datos, Comercio electrónico y Firma Digital.[55]

2000. Resolución 270/2000, de 4 de marzo de 2000, por la cual se Dictan Normas sobre Protección a los Usuarios para la Prestación de Servicios Públicos No Domiciliarios de Telecomunicaciones.

Decreto 1747 de 11 de septiembre de 2000, por el cual se reglamenta parcialmente la ley 527 certificados y firmas digitales.

Resolución 7652/2000, de 22 de septiembre de la Dirección General de Impuestos y Aduanas Nacionales, por la cual se reglamenta la administración,

---

[51] LEGISLACIÓN INFORMÁTICA DE COLOMBIA. Ley de Protección de datos de 1988. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: Informática Jurídica website: http://www.informatica-juridica.com/legislacion/colombia/

[52] DIRECCIÓN NACIONAL DEL DERECHO DE AUTOR. Decreto 1360, de 23 de junio de 1989. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://propiedadintelectual.unal.edu.co. recursos>docs>normatividad

[53] LEGISLACIÓN INFORMÁTICA DE COLOMBIA. Decreto 1900 de 1990. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.informatica-juridica.com.>legislacion-informatica

[54] _____. Decreto 2150 de 1995. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.informatica-juridica.com.>legislacion-informatica

[55] _____. Ley 527 de agosto 18 de 1999. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.informatica-juridica.com.>legislacion-informatica

publicación y uso de la información electrónica vía INTRANET e INTERNET en la Dirección de Impuestos y Aduanas Nacionales. [56]

2001. Proyecto de Ley 35 de 2001 Cámara. Aspectos jurídicos de los servicios de la sociedad de la información, en desarrollo del Comercio Electrónico.[57]

Ley 679 de 3 de agosto de 2001 sobre Abuso y pornografía de menores en Internet. (Diario Oficial número 44509 del 4 de agosto de 2001).[58]

2002. Decreto 55 de 15 de febrero de 2002 de la Alcaldía Mayor de Bogotá, por medio del cual se establece "El Sistema de Declaración y Pago de Impuestos Distritales a través de medios electrónicos".[59]

Resolución 600/2002 de 7 de mayo, del Ministerio de Comunicaciones, por medio de la cual se regula parcialmente la administración del dominio punto .com.[60]

2003. Resolución 20/2003, de 14 de enero, del Ministerio de Comunicaciones, por medio de la cual se establece el procedimiento a seguir por el Ministerio de Comunicaciones para la fijación de las condiciones de administración del dominio.co.[61]

2004. Ley 890 de 7 de julio de 2004, por la cual se modifica y adiciona el Código Penal (Diario Oficial nº 45.602, de 7 de julio de 2004)[62].

Ley 892 de 7 de julio 2004. Voto electrónico[63].

---

[56] LEGISLACIÓN INFORMÁTICA DE COLOMBIA. Resolución 7652/2000, de 22 de septiembre [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

[57] _____. Ley 35 de 2001. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

[58] _____. Ley 679 de 3 de agosto de 2001. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

[59] _____. Decreto 55 de febrero 15 de 2002 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

[60] _____. Resolución 600/2002 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

[61] _____. Resolución 20 de 2003 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

[62] LEGISLACION INFORMATICA DE COLOMBIA. Ley 890 de 7 de julio de 2004. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

[63] _____. Ley 892 de 7 de julio 2004. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

2005. Resolución 1271 de 24 de junio de 2005 del Ministerio de Comercio, Industria y Turismo, por la cual se fija el precio de los aplicativos informáticos para su transmisión a la Ventanilla Única de Comercio Exterior – VUCE – .[64]

Ley 962 de 8 de Julio de 2005, por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.[65]

2006. Acuerdo nº PSAA06-3334 de 2 de marzo de 2006 del Consejo Superior de la Judicatura, por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia.

Proyecto de Ley 05/2006 Senado "Por el cual se reglamenta el Habeas Data y el Derecho de Petición ante Entidades Financieras, Bancarias y Centrales o Banco de Datos". [66]

2007. Informe de Conciliación al Proyecto de Ley Estatutaria 221/2007 de 4 de junio de 2007, sobre el Derecho de Habeas Data.

Resolución 1732 de 17 de septiembre de 2007, de la Comisión de Regulación de Telecomunicaciones, por la cual se expide el Régimen de Protección de los Derechos de los Suscriptores y/o Usuarios de los Servicios de Telecomunicaciones.[67]

2008. Ley 1221 de 16 de julio de 2008, por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones[68]

Ley 1266 de 31 de diciembre de 2008, por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.[69] (Diario Oficial nº 47.219).

---

[64] MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Resolución 1271 de 24 de junio de 2004. En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.mincit.gov.co.Resolucion-1271-del-24-de junio-de-2005.

[65] FUNCION PÚBLICA. Ley 962 de julio 8 de 2005. Colombia: Diario Oficial 45963, 2005. 17 p,

[66] CONSEJO SUPERIOR DE LA JUDICATURA. Acuerdo nº PSAA06-3334 de 2 de marzo de 2006. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://normograma.info>docs>pdf> acuerdo__csjudicatura_3334_2006

[67] COMISION DE REGULACION DE TELECOMUNICACIONES. Resolución 1732 de 17 de sep. De 2007. Colombia: Diario Oficial No. 46.756. 2007. 58 p.

[68] RED NACIONAL DE FOMENTO AL TELETRABAJO. Ley 1221 de julio 16 de 2008. Diario Oficial No. 47052. 2007. 58 p.

[69] CORTE CONSTITUCIONAL. Ley 1266 de 31 de diciembre de 2008. Colombia: Diario Oficial nº 47.219. 2008. 9 p.

2009. Ley 1273 de 5 de enero de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Diario Oficial nº 47.223).

2010. Resolución 2347 de 26 de enero de 2010 CRC, de la Comisión de Regulación de las Comunicaciones, con la que se establecen disposiciones en materia de protección de los derechos de usuarios respecto de tarifas de telefonía pública básica conmutada.

Resolución 2554 de 19 de mayo de 2010 CRC, de la Comisión de Regulación de las Comunicaciones, Modificación al Régimen de Protección de los Derechos de los Usuarios de Servicios de Telecomunicaciones.

2011. Proyecto de Ley de abril de 2011 por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet.

Lineamientos de política para Ciberseguridad y Ciberdefensa de 14 de julio de 2011.

2012. Ley Estatutaria 1581 de 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de los datos personales (Diario Oficial nº 48.587 de 18 de octubre de 2012)

Decreto 2364 de 22 de noviembre de 2012, sobre la firma electrónica.

2013. Ley nº 1680 de 20 de noviembre de 2013, por la cual se garantiza a las personas ciegas y con baja visión, el acceso a la información, a las comunicaciones, al conocimiento y a las tecnologías de la información y de las comunicaciones. (Diario Oficial nº 48.980 de 20 de noviembre de 2013).

2014. Ley 1712 de 6 de marzo de 2014, por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información Pública Nacional y se dictan otras disposiciones. (Diario Oficial nº 49.084 de 6 de marzo de 2014).

Decreto 2573 de 12 de diciembre de 2014, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. (Publicado en el Diario Oficial 49363 de 12 de diciembre de 2014).

2015. Resolución 4841 de 30 de diciembre de 2015, de la Comisión de Regulación de Comunicaciones, por la cual se complementan y modifican las

condiciones generales para la provisión de infraestructura de las redes de televisión abierta radiodifundida.

2016. Proyecto de Ley número 94, de 10 de agosto de 2016 Senado: Por medio del cual se busca modificar y adicionar la Ley Estatutaria 1266 de 2008, y se dictan disposiciones de hábeas data relacionadas con información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Resolución 5050 de 10 de noviembre de 2016, de la Comisión de Regulación de Comunicaciones, por la cual de compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones.

2017. Resolución 5111 de 24 de febrero de 2017, de la Comisión de Regulación de Comunicaciones, por la cual se establece el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones y se modifica el Capítulo 1 del Título II de la Resolución CRC 5050 de 10 de noviembre de 2016 y se dictan otras disposiciones.

Resolución 670 de 14 de diciembre de 2017, de la Procuraduría General de la Nación, por medio de la cual se adopta el manual de políticas y procedimientos para la protección de datos personales.

2018. Ley 1928 de 24 de julio de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

Proyecto de Ley Estatutaria nº de 2018, por medio de la cual se modifica y adiciona la Ley Estatutaria 1266 de 2008, y se dictan disposiciones generales del Hábeas Data con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.[70]

2019. Circular externa nº 1, de 16 de enero de 2019, de la Superintendencia de Industria y Comercio de Colombia, sobre la obligación de registro de bases de datos.

[70] LEGISLACION INFORMATICA DE COLOMBIA. Proyecto de ley estatutaria No. 1266. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

4. DISEÑO METODOLÓGICO

Para el análisis de riesgos desplegado en el servidor de proyectos se aplicó la metodología MAGERIT, la cual permite en sus diferentes fases mostrar cómo se encuentran los activos de la institución en cuanto a riesgos y proporciona elementos para tratar dichos riesgos encontrados.

Para este análisis fue fundamental el uso de la herramienta EAR/PILAR, el cual es un software potente basado en Magerit.

Las fases de la metodología son las siguientes:

4.1 ANÁLISIS DE ACTIVOS

En esta fase se identifican los activos de la institución. Esta fase se divide en las siguientes sub-fases:

4.1.1 Tipo de activos. No todos los activos son de la misma clasificación. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes.

Los tipos de activos se clasifican de la siguiente manera:

- SW: Software
- HW: Hardware
- B: Activos esenciales
- E: Equipamiento
- AUX: Elementos auxiliares
- L: Instalaciones

4.1.1.1 Dimensiones. De un activo puede interesar calibrar diferentes dimensiones:

- Su autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)

- Su confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.

- Su integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.

- Su disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

- Su trazabilidad del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

- Su trazabilidad del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

4.1.1.2 Valoración de los activos. No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

4.1.1.3 Análisis de amenazas. En esta fase se listan todas aquellas situaciones denominadas amenazas que atenten contra la integridad de la institución. Esta fase se divide en las siguientes sub-fases:

Clasificación de amenazas

- **De origen natural.** Hay accidentes naturales (terremotos, inundaciones). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

- **Del entorno (de origen industrial).** Hay desastres industriales (contaminación, fallos eléctricos) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

- **Defectos de las aplicaciones**. Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades’.

- **Causadas por las personas de forma accidental**. Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

- **Causadas por las personas de forma deliberada**. Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

- **Identificación de amenazas.** Se listan todas las amenazas que puedan causar afectaciones sobre los activos identificados.

- **Valoración de Amenazas.** Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

– Degradación: cuán perjudicado resultaría el [valor del] activo.

– Probabilidad: cuán probable o improbable es que se materialice la amenaza La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

4.2 DETERMINACIÓN DEL IMPACTO POTENCIAL

4.2.1 Clasificación del impacto potencial. Se establece una valoración de acuerdo al nivel del impacto.

4.2.2 Identificación del impacto potencial. Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

4.3 DETERMINACIÓN DEL RIESGO POTENCIAL

4.3.1 Clasificación del riesgo potencial. Se establece una valoración de acuerdo al nivel de criticidad del riesgo.

4.3.2 Identificación del riesgo potencial. Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

4.4 ANÁLISIS DE SALVAGUARDAS

4.4.1 Clasificación de salvaguardas. Se clasifican las salvaguardas para saber de qué tipo son, y cómo influyen en la empresa.

4.4.2 Identificación de salvaguardas. En esta fase se identifican las salvaguardas de acuerdo a las amenazas y riesgos potenciales detectados.

4.5 DETERMINACIÓN DEL IMPACTO RESIDUAL

4.5.1 Clasificación del Impacto Potencial. Se establece una valoración de acuerdo al nivel del impacto.

4.5.2 Identificación del impacto residual. Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

4.6 DETERMINACIÓN DEL RIESGO RESIDUAL

4.6.1 Clasificación del riesgo residual. Se establece una valoración de acuerdo al nivel de criticidad del riesgo.

4.6.2 Identificación del riesgo residual. Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

4.7 RECURSOS

4.7.1 Recursos materiales e institucionales. Los costos de Equipos y software y bibliografía, no implican un gasto considerable ya que el acceso a los computadores se realizará desde el domicilio, o desde las instalaciones de la UNAD. Así mismo, el acceso a los recursos bibliográficos se hará por medio de la Universidad Nacional de Colombia, el cual es gratuito para egresados de esta universidad.

Los costos, respecto al recurso humano que participe en el proyecto, implican gasto de dinero bajos, casi nulos, ya que esta participación hace parte del ejercicio académico, sin requerimiento de una vinculación laboral, por lo que tampoco implicará gasto de dinero.

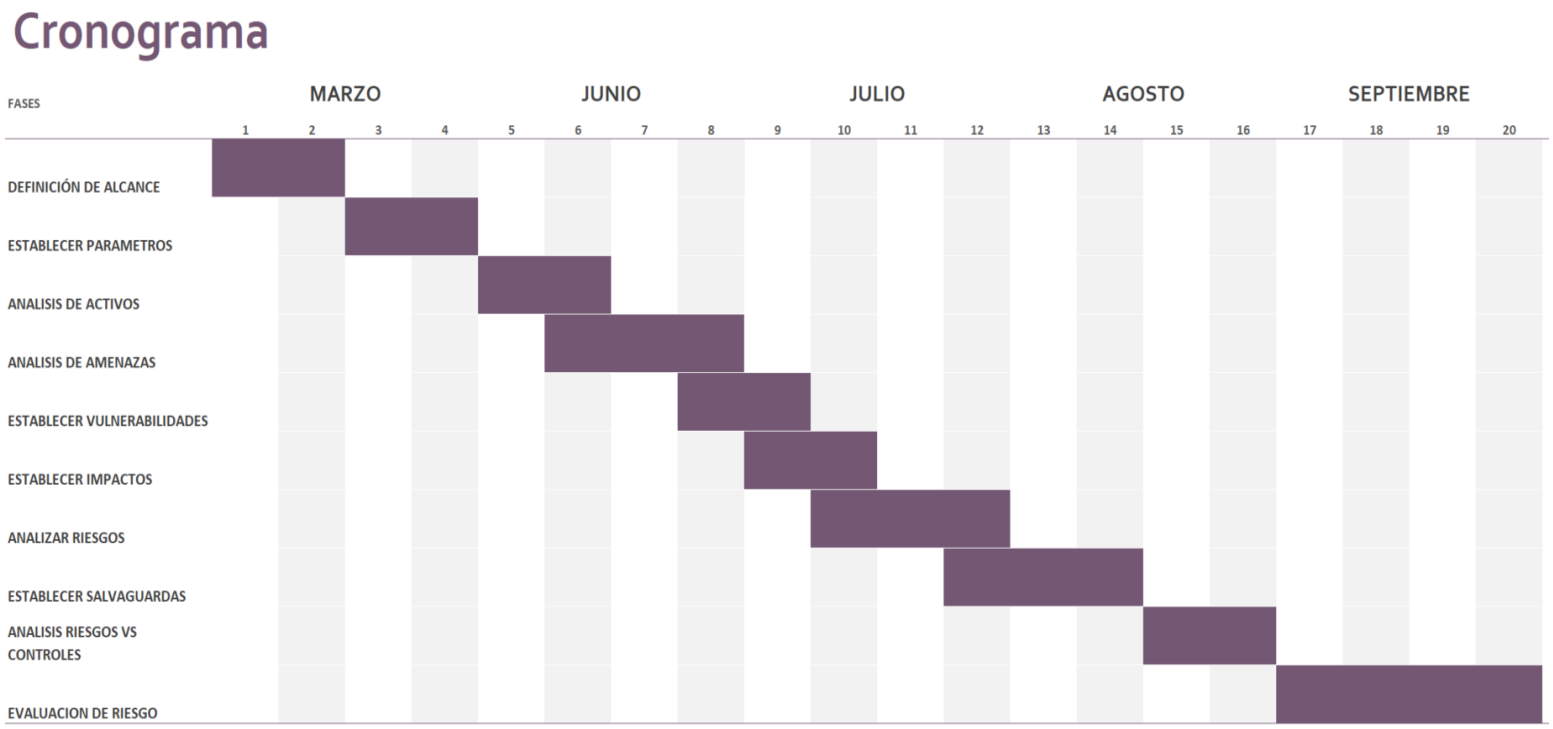
Tabla 1. Recursos utilizados

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	**Director del proyecto. Ingeniero de Sistemas Jefe de infraestructura-Empresa**	**Recursos propios**
Equipos y Software	**Computadores propios. La UNAD apoyo esta iniciativa con equipos para consulta de información.**	**2.500.000**
Viajes y Salidas	**Viajes para acceder a los servidores remoto y presencial**	**300.000**
Materiales y suministros	**Software Opensource**	**Recursos propios**
Bibliografía	**Bases de datos**	**Acceso a biblioteca de la UNAD y de la Universidad Nacional de Colombia**

Fuente: autor

4.8 CRONOGRAMA

Tabla 2 Cronograma del Proyecto.



Fuente: autor

5. DESARROLLO DEL PROYECTO

5.1 ANÁLISIS DE ACTIVOS

Se realizó la identificación de los activos esenciales dentro del alcance del proyecto y se clasificaron de acuerdo al tipo de activo.

5.1.1 Tipo de activos

[INF1] INFORMACIÓN DE LA EMPRESA: Datos confidenciales de la empresa que se guardan en los servidores.

[SW] Aplicaciones

- [SW1] FROZEN: Plataforma Web para la gestión administrativa alojada en los servidores web.

- [SW2] ICEBERG: Plataforma para la gestión financiera alojada en los servidores web

[HW] Equipos

- [HW1] SERVIDOR 1: Servidor que apoya diferentes plataformas de gestión, donde se encuentra gran parte de la información de la empresa.

- [HW2] SERVIDOR 2: Servidor que apoya en servidor 1 en la temática de backups e implementación de pruebas.

[AUX] Elementos auxiliares

- [AUX1] UPS: Es un dispositivo que proporciona energía eléctrica por un tiempo limitado a todos los equipos que estén conectados a cierta red eléctrica, durante un apagón.

[L] Instalaciones

- [L1] Centro de Cableado: La zona de cableado es el lugar donde se crean las redes de **área** local.

5.2 DIMENSIONES

[D] Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. («Norma UNE 71504:2008», s. f.)

[I] Integridad de los datos: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. («Norma UNE 71504:2008», s. f.)

[C] Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. («Norma UNE 71504:2008», s. f.)

[A] Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. («Norma UNE 71504:2008», s. f.)

[T] Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. («Norma UNE 71504:2008», s. f.)

[V] Valor: Propiedad o característica consistente en el valor que tienen los activos para la empresa, en específico, si corresponde a patrimonio de la misma. («Norma UNE 71504:2008», s. f.)

[DP] Datos Personales: Propiedad o característica consistente en los datos confidenciales de la empresa. («Norma UNE 71504:2008», s. f.)

5.3 VALORACION DE LOS ACTIVOS

Para cada valoración se debe tener en cuenta la siguiente información:

- Criterios de valoración
- Dimensiones (Ver numeral 4.2)

Tabla 3. Escalas de valoración de activos

VALOR		CRITERIO
10	EXTREMO	Daño extremadamente grave.
9	MUY ALTO	Daño muy grave.
6-8	ALTO	Daño grave.
3-5	MEDIO	Daño importante.
1-2	BAJO	Daño menor.
0	DESPRECIABLE	Irrelevante.

Fuente: autor

Tabla 4. Valoración de activos

ACTIVOS	DIMENSIONES						
	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[INF1] INFORMACIÓN DE LA EMPRESA	9	7	7		7	9	6
[SW] Aplicaciones							
[SW1] FROZEN	7	7	7	7	7	6	[n.a]
[SW2] ICEBERG	7	7	7	7	7	6	[n.a]
[HW] Equipos							
[HW1] SERVIDOR 1	7	6	8	7	7	6	6
[HW2] SERVIDOR 2	7	6	8	7	7	6	6
[AUX] Elementos auxiliares							
[AUX1] UPS	8	6	[n.a]	[n.a]	[n.a]	6	[n.a]
[L] Instalaciones							
[L1] Centro de Cableado	7	7	7	7	[n.a]	6	[n.a]

Fuente: autor

5.4 ANÁLISIS DE AMENAZAS

En esta fase se detectaron todas las amenazas a las que se encuentran expuestos los activos.

5.4.1 Clasificación de las amenazas

[PR.g1] De origen normativo
[N] Desastres Natural
[I] De origen industrial
[E] Errores y fallos no intencionados
[A] Ataque intencionados

5.4.2 Identificación de las amenazas. Se listan todas las amenazas que puedan causar afectaciones sobre los activos identificados.

Tabla 5. Identificación de amenazas

ACTIVO	AMENAZA
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g1] 1. No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g2] 2. Tratar datos inadecuados y excesivos para la finalidad del tratamiento
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g3] 3. Carecer de una base jurídica sobre la que se sustenten los tratamientos realizados sobre los datos
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g4] 4. Tratar datos personales con una finalidad distinta para la cual fueron recabados
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g5] 5. No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la privacidad en la organización
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g6] 6. Almacenar los datos por periodos superiores a los necesarios para la finalidad del tratamiento y a la legislación vigente
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g7] 7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g10] 10. Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g11] 11. Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado el tratamiento
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g12] 12. No registrar la creación, modificación o cancelación de las actividades de tratamiento efectuadas bajo su responsabilidad
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g13] 13. No llevar a cabo por parte del responsable del tratamiento una evaluación de impacto adecuada en los supuestos detallados por la normativa aplicable
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g24] 24. Información no actualizada o incorrecta (pe. registros duplicados con informaciones contradictorias o con campos de datos incorrectos)
Tabla 5. Continuación	
[SW1] FROZEN, [SW2] ICEBERG	[I.5] Avería de origen físico o lógico
[SW1] FROZEN, [SW2] ICEBERG	[E.8] Difusión de software dañino

ACTIVO	AMENAZA
[SW1] FROZEN, [SW2] ICEBERG	[E.20] Vulnerabilidades de los programas (software)
[SW1] FROZEN, [SW2] ICEBERG	[E.21] Errores de mantenimiento / actualización de programas (software)
[SW1] FROZEN, [SW2] ICEBERG	[A.8] Difusión de software dañino
[SW1] FROZEN, [SW2] ICEBERG	[A.22] Manipulación de programas
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.1] Fuego
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.2] Daños por agua
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.*] Desastres naturales
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.1] Fuego
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.2] Daños por agua
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.*] Desastres industriales
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.3] Contaminación medioambiental
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.4] Contaminación electromagnética
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.5] Avería de origen físico o lógico
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.6] Corte del suministro eléctrico
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.7] Condiciones inadecuadas de temperatura o humedad
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.11] Emanaciones electromagnéticas
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.24] Caída del sistema por agotamiento de recursos
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.25] Pérdida de equipos
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.11] Acceso no autorizado
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.23] Manipulación del hardware
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.24] Denegación de servicio
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.25] Robo de equipos
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.26] Ataque destructivo
[AUX1] UPS	[N.1] Fuego
[AUX1] UPS	[N.2] Daños por agua
[AUX1] UPS	[N.*] Desastres naturales
Tabla 5. continuación	
[AUX1] UPS	[I.1] Fuego
[AUX1] UPS	[I.2] Daños por agua
[AUX1] UPS	[I.*] Desastres industriales
[AUX1] UPS	[I.3] Contaminación medioambiental

ACTIVO	AMENAZA
[AUX1] UPS	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[AUX1] UPS	[A.7] Uso no previsto
[AUX1] UPS	[A.23] Manipulación del hardware
[AUX1] UPS	[A.25] Robo de equipos
[AUX1] UPS	[A.26] Ataque destructivo
[L1] Centro de Cableado	[N.1] Fuego
[L1] Centro de Cableado	[N.2] Daños por agua
[L1] Centro de Cableado	[N.*] Desastres naturales
[L1] Centro de Cableado	[I.1] Fuego
[L1] Centro de Cableado	[I.2] Daños por agua
[L1] Centro de Cableado	[I.*] Desastres industriales
[L1] Centro de Cableado	[I.3] Contaminación medioambiental
[L1] Centro de Cableado	[I.4] Contaminación electromagnética
[L1] Centro de Cableado	[I.8] Fallo de servicios de comunicaciones
[L1] Centro de Cableado	[E.2] Errores del administrador del sistema / de la seguridad
[L1] Centro de Cableado	[E.9] Errores de [re-]encaminamiento
[L1] Centro de Cableado	[E.10] Errores de secuencia
[L1] Centro de Cableado	[E.15] Alteración de la información
[L1] Centro de Cableado	[E.19] Fugas de información
[L1] Centro de Cableado	[E.24] Caída del sistema por agotamiento de recursos
[L1] Centro de Cableado	[A.5] Suplantación de la identidad
[L1] Centro de Cableado	[A.6] Abuso de privilegios de acceso
[L1] Centro de Cableado	[A.7] Uso no previsto
[L1] Centro de Cableado	[A.9] [Re-]encaminamiento de mensajes
[L1] Centro de Cableado	[A.10] Alteración de secuencia
[L1] Centro de Cableado	[A.11] Acceso no autorizado
[L1] Centro de Cableado	[A.12] Análisis de tráfico
[L1] Centro de Cableado	[A.14] Interceptación de información (escucha)
[L1] Centro de Cableado	[A.15] Modificación de la información
[L1] Centro de Cableado	[A.18] Destrucción de la información
[L1] Centro de Cableado	[A.24] Denegación de servicio
[L1] Centro de Cableado	[A.26] Ataque destructivo
[L1] Centro de Cableado	[A.27] Ocupación enemiga

Fuente: autor

5.4.3 Valoración de las amenazas. La probabilidad de ocurrencia es más compleja de determinar y de expresar. A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra. Son valores típicos:

Tabla 6. Probabilidad de ocurrencia

PROBABILIDAD DE OCURRENCIA		
100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
0,1	Poco Frecuente	Cada varios años
0,01	Muy Poco Frecuente	Siglos

Fuente: autor

Tabla 7. Escalas de degradación de un activo

DEGRADACIÓN DEL VALOR		
MA	100%	Muy Alta
A	90%	Alta
M	50%	Media
B	20%	Baja
MB	10%	Muy Baja
E	1%	Escasa

Fuente: autor

Tabla 8. Valoración Activos VS Amenazas

ACTIVO	Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g1]	10	-	-	-	-	-	-	20%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g2]	10	-	-	-	-	-	-	50%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g3]	10	-	-	-	-	-	-	50%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g4]	10	-	-	-	-	-	-	90%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g5]	5	-	-	-	-	-	-	50%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g6]	10	-	-	-	-	-	-	50%
Tabla 8. Continuación									
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g7]	10	-	-	-	-	-	-	90%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g8]	10	-	-	-	-	-	-	100%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g9]	10	-	-	-	-	-	-	100%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g10]	10	-	-	-	-	-	-	90%

ACTIVO	Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g11]	10	-	-	-	-	-	-	90%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g12]	5	-	-	-	-	-	-	50%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g13]	5	-	-	-	-	-	-	50%
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g14]	10	-	-	-	-	-	-	50%
[SW1] FROZEN, [SW2] ICEBERG	[I.5]	1	50%	-	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.8]	1	10%	10%	10%	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.20]	1	1%	20%	20%	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.21]	10	1%	1%	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[A.8]	1	100%	100%	100 %	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[A.22]	1	50%	100%	100 %	-	-	-	-
ACTIVO	amenaza	frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.1]	0	100%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.2]	0	50%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.*]	0	100%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.1]	1	100%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.2]	1	50%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.*]	1	100%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.3]	0	50%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.4]	1	10%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.5]	1	50%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.6]	1	100%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.7]	1	100%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.11]	1	-	-	1%	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.23]	1	10%	-	-	-	-	-	-
Tabla 8. Continuación									
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.24]	10	50%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.25]	1	100%	-	50%	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.11]	1	10%	10%	50%	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.23]	1	50%	-	50%	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.24]	2	100%	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.25]	1	100%	-	50%	-	-	-	-
[HW1] SERVIDOR 1, [HW2]	[A.26]	1	100%	-	-	-	-	-	-

ACTIVO	Amenaza	Frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
SERVIDOR 2									
[AUX1] UPS	[N.1]	0	100%	-	-	-	-	-	-
[AUX1] UPS	[N.2]	0	50%	-	-	-	-	-	-
[AUX1] UPS	[N.*]	0	100%	-	-	-	-	-	-
[AUX1] UPS	[I.1]	1	100%	-	-	-	-	-	-
[AUX1] UPS	[I.2]	1	50%	-	-	-	-	-	-
[AUX1] UPS	[I.*]	1	100%	-	-	-	-	-	-
[AUX1] UPS	[I.3]	0	50%	-	-	-	-	-	-
[AUX1] UPS	[E.23]	1	10%	-	-	-	-	-	-
[AUX1] UPS	[A.7]	1	50%	1%	-	-	-	-	-
[AUX1] UPS	[A.23]	1	50%	-	-	-	-	-	-
[AUX1] UPS	[A.25]	1	10%	-	-	-	-	-	-
[AUX1] UPS	[A.26]	1	10%	-	-	-	-	-	-
ACTIVO	amenaza	frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L1] Centro de Cableado	[N.1]	1	100%	-	-	-	-	-	-
[L1] Centro de Cableado	[N.2]	1	100%	-	-	-	-	-	-
[L1] Centro de Cableado	[N.*]	1	100%	-	-	-	-	-	-
[L1] Centro de Cableado	[I.1]	1	100%	-	-	-	-	-	-
[L1] Centro de Cableado	[I.2]	1	100%	-	-	-	-	-	-
[L1] Centro de Cableado	[I.*]	1	100%	-	-	-	-	-	-
[L1] Centro de Cableado	[I.3]	1	10%	-	-	-	-	-	-
[L1] Centro de Cableado	[I.4]	0	10%	-	-	-	-	-	-
[L1] Centro de Cableado	[I.8]	1	50%	-	-	-	-	-	-
[L1] Centro de Cableado	[E.2]	1	20%	20%	20%	-	-	-	-
[L1] Centro de Cableado	[E.9]	1	-	-	10%	-	-	-	-
[L1] Centro de Cableado	[E.10]	1	-	10%	-	-	-	-	-
[L1] Centro de Cableado	[E.15]	1	-	1%	-	-	-	-	-
[L1] Centro de Cableado	[E.19]	1	-	-	10%	-	-	-	-
[L1] Centro de Cableado	[E.24]	1	50%	-	-	-	-	-	-
[L1] Centro de Cableado	[A.5]	1	-	10%	50%	100%	-	-	-
[L1] Centro de Cableado	[A.6]	1	10%	-	-	-	-	-	-
Tabla 8. Continuación									
[L1] Centro de Cableado	[A.7]	1	10%	10%	10%	-	-	-	-
[L1] Centro de Cableado	[A.9]	1	-	-	10%	-	-	-	-
[L1] Centro de Cableado	[A.10]	1	-	10%	-	-	-	-	-
[L1] Centro de Cableado	[A.11]	1	-	10%	50%	100%	-	-	-
[L1] Centro de Cableado	[A.12]	1	-	-	2%	-	-	-	-
[L1] Centro de Cableado	[A.14]	1	-	-	10%	-	-	-	-
[L1] Centro de Cableado	[A.15]	1	-	10%	-	-	-	-	-
[L1] Centro de Cableado	[A.18]	1	50%	-	-	-	-	-	-
[L1] Centro de Cableado	[A.24]	10	50%	-	-	-	-	-	-
[L1] Centro de Cableado	[A.26]	0	100%	-	-	-	-	-	-

Fuente: autor

5.5 DETERMINACIÓN DEL IMPACTO POTENCIAL

5.5.1 Clasificación del impacto potencial. El impacto potencial se muestra en la siguiente escala con colores que indican su severidad.

Tabla 9. Escala de impacto potencial

VALORACION	CRITERIO
[10]	Nivel 10
[9]	Nivel 9
[8]	Alto (+)
[7]	Alto
[6]	Alto (-)
[5]	Medio (+)
[4]	Medio
[3]	Medio (-)
[2]	Bajo (+)
[1]	Bajo
[0]	Despreciable
Fuente: autor	

5.5.2 Identificación del impacto potencial

Tabla 10. Valoración Impacto Potencial

ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g1]	-	-	-	-	-	-	4
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g2]	-	-	-	-	-	-	5
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g3]	-	-	-	-	-	-	5
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g4]	-	-	-	-	-	-	6
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g5]	-	-	-	-	-	-	5
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g6]	-	-	-	-	-	-	5
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g7]	-	-	-	-	-	-	6
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g8]	-	-	-	-	-	-	6
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g9]	-	-	-	-	-	-	6
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g10]	-	-	-	-	-	-	6
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g11]	-	-	-	-	-	-	6
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g12]	-	-	-	-	-	-	5
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g13]	-	-	-	-	-	-	5
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g14]	-	-	-	-	-	-	5
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[SW1] FROZEN, [SW2] ICEBERG	[I.5]	8	-	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.8]	6	4	4	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.20]	3	5	5	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.21]	3	1	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[A.8]	9	7	7	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[A.22]	8	7	7	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.1]	9	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.2]	8	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.*]	9	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.1]	9	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.2]	8	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.*]	9	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.3]	8	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.4]	6	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.5]	8	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.6]	9	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.7]	9	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.11]	-	-	1	-	-	-	-
Tabla 10. Continuación								
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.23]	6	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.24]	8	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.25]	9	-	6	-	-	-	-

ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.11]	6	4	6	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.23]	8	-	6	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.24]	9	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.25]	9	-	6	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.26]	9	-	-	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[AUX1] UPS	[N.1]	9	-	-	-	-	-	-
[AUX1] UPS	[N.2]	8	-	-	-	-	-	-
[AUX1] UPS	[N.*]	9	-	-	-	-	-	-
[AUX1] UPS	[I.1]	9	-	-	-	-	-	-
[AUX1] UPS	[I.2]	8	-	-	-	-	-	-
[AUX1] UPS	[I.*]	9	-	-	-	-	-	-
[AUX1] UPS	[I.3]	8	-	-	-	-	-	-
[AUX1] UPS	[E.23]	6	-	-	-	-	-	-
[AUX1] UPS	[A.7]	8	1	1	-	-	-	-
[AUX1] UPS	[A.23]	8	-	6	-	-	-	-
[AUX1] UPS	[A.25]	6	-	-	-	-	-	-
[AUX1] UPS	[A.26]	6	-	-	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L1] Centro de Cableado	[N.1]	9	-	-	-	-	-	-
[L1] Centro de Cableado	[N.2]	9	-	-	-	-	-	-
[L1] Centro de Cableado	[N.*]	9	-	-	-	-	-	-
[L1] Centro de Cableado	[I.1]	9	-	-	-	-	-	-
[L1] Centro de Cableado	[I.2]	9	-	-	-	-	-	-
[L1] Centro de Cableado	[I.*]	9	-	-	-	-	-	-
[L1] Centro de Cableado	[I.3]	6	-	-	-	-	-	-
[L1] Centro de Cableado	[I.4]	6	-	-	-	-	-	-
[L1] Centro de Cableado	[I.8]	8	-	-	-	-	-	-
[L1] Centro de Cableado	[E.2]	7	5	5	-	-	-	-
[L1] Centro de Cableado	[E.9]	-	-	4	-	-	-	-
[L1] Centro de Cableado	[E.10]	-	4	-	-	-	-	-
[L1] Centro de Cableado	[E.15]	-	1	-	-	-	-	-
[L1] Centro de Cableado	[E.19]	-	-	4	-	-	-	-
[L1] Centro de Cableado	[E.24]	8	-	-	-	-	-	-
[L1] Centro de Cableado	[A.5]	-	4	6	7	-	-	-
[L1] Centro de Cableado	[A.6]	6	-	-	-	-	-	-
[L1] Centro de Cableado	[A.7]	6	4	4	-	-	-	-
Tabla 10. Continuación								
[L1] Centro de Cableado	[A.9]	-	-	4	-	-	-	-
[L1] Centro de Cableado	[A.10]	-	4	-	-	-	-	-
[L1] Centro de Cableado	[A.11]	-	4	6	7	-	-	-
[L1] Centro de Cableado	[A.12]	-	-	2	-	-	-	-

ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L1] Centro de Cableado	[A.14]	-	-	4	-	-	-	-
[L1] Centro de Cableado	[A.15]	-	4	-	-	-	-	-
[L1] Centro de Cableado	[A.18]	8	-	-	-	-	-	-
[L1] Centro de Cableado	[A.24]	8	-	-	-	-	-	-
[L1] Centro de Cableado	[A.26]	8	-	-	-	-	-	-
[L1] Centro de Cableado	[A.27]	9	-	-	-	-	-	-

Fuente: autor

5.6 DETERMINACIÓN DEL RIESGO POTENCIAL

5.6.1 Clasificación del riesgo potencial. El riesgo potencial se muestra en la siguiente escala con colores que indican su criticidad.

Tabla 11. Escala Riesgo Potencial

ESCALA DE RIESGO	
VALORACION	CRITERIO
[9]	Nivel 9
[8]	Alto (+)
[7]	Alto
[6]	Alto (-)
[5]	Medio (+)
[4]	Medio
[3]	Medio (-)
[2]	Bajo (+)
[1]	Bajo
[0]	Despreciable

Fuente: autor

5.6.2 Identificación del riesgo potencial

Tabla 12. Valoración Riesgo Potencial

ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g1]	-	-	-	-	-	-	{4.1}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g2]	-	-	-	-	-	-	{4.8}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g3]	-	-	-	-	-	-	{4.8}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g4]	-	-	-	-	-	-	{5.3}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g5]	-	-	-	-	-	-	{4.6}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g6]	-	-	-	-	-	-	{4.8}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g7]	-	-	-	-	-	-	{5.3}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g8]	-	-	-	-	-	-	{5.4}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g9]	-	-	-	-	-	-	{5.4}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g10]	-	-	-	-	-	-	{5.3}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g11]	-	-	-	-	-	-	{5.3}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g12]	-	-	-	-	-	-	{4.6}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g13]	-	-	-	-	-	-	{4.6}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g14]	-	-	-	-	-	-	{4.8}
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[SW1] FROZEN, [SW2] ICEBERG	[I.5]	{5.7}	-	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.8]	{4.5}	{3.3}	{3.3}	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.20]	{2.7}	{3.8}	{3.8}	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.21]	{3.6}	{2.4}	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[A.8]	{6.2}	{5.1}	{5.1}	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[A.22]	{5.7}	{5.1}	{5.1}	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.1]	{5.4}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.2]	{4.8}	-	-	-	-	-	-
Tabla 12. Continuación								
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.*]	{5.4}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.1]	{6.0}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.2]	{5.4}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.*]	{6.0}	-	-	-	-	-	-

ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.3]	{4.8}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.4]	{4.5}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.5]	{5.7}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.6]	{6.2}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.7]	{6.2}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.11]	-	-	{2.1}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.23]	{4.5}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.24]	{6.6}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.25]	{6.2}	-	{5.1}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.11]	{4.5}	{3.3}	{5.1}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.23]	{5.4}	-	{4.9}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.24]	{6.5}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.25]	{6.0}	-	{4.9}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.26]	{6.2}	-	-	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[AUX1] UPS	[N.1]	{5.4}	-	-	-	-	-	-
[AUX1] UPS	[N.2]	{4.8}	-	-	-	-	-	-
[AUX1] UPS	[N.*]	{5.4}	-	-	-	-	-	-
[AUX1] UPS	[I.1]	{6.0}	-	-	-	-	-	-
[AUX1] UPS	[I.2]	{5.4}	-	-	-	-	-	-
[AUX1] UPS	[I.*]	{6.0}	-	-	-	-	-	-
[AUX1] UPS	[I.3]	{4.8}	-	-	-	-	-	-
[AUX1] UPS	[E.23]	{4.5}	-	-	-	-	-	-
[AUX1] UPS	[A.7]	{5.7}	{1.5}	{1.5}	-	-	-	-
Tabla 12. Continuación								
[AUX1] UPS	[A.23]	{5.7}	-	{4.5}	-	-	-	-
[AUX1] UPS	[A.25]	{4.2}	-	-	-	-	-	-
[AUX1] UPS	[A.26]	{4.5}	-	-	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L1] Centro de Cableado	[N.1]	{6.2}	-	-	-	-	-	-
[L1] Centro de Cableado	[N.2]	{6.2}	-	-	-	-	-	-
[L1] Centro de Cableado	[N.*]	{6.0}	-	-	-	-	-	-
[L1] Centro de Cableado	[I.1]	{6.2}	-	-	-	-	-	-

ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L1] Centro de Cableado	[I.2]	{6.2}	-	-	-	-	-	-
[L1] Centro de Cableado	[I.*]	{6.2}	-	-	-	-	-	-
[L1] Centro de Cableado	[I.3]	{4.5}	-	-	-	-	-	-
[L1] Centro de Cableado	[I.4]	{3.6}	-	-	-	-	-	-
[L1] Centro de Cableado	[I.8]	{5.7}	-	-	-	-	-	-
[L1] Centro de Cableado	[E.2]	{5.0}	{3.8}	{3.8}	-	-	-	-
[L1] Centro de Cableado	[E.9]	-	-	{3.3}	-	-	-	-
[L1] Centro de Cableado	[E.10]	-	{3.3}	-	-	-	-	-
[L1] Centro de Cableado	[E.15]	-	{1.5}	-	-	-	-	-
[L1] Centro de Cableado	[E.19]	-	-	{3.3}	-	-	-	-
[L1] Centro de Cableado	[E.24]	{5.7}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.5]	-	{3.3}	{4.5}	{5.1}	-	-	-
[L1] Centro de Cableado	[A.6]	{4.5}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.7]	{4.5}	{3.3}	{3.3}	-	-	-	-
[L1] Centro de Cableado	[A.9]	-	-	{3.3}	-	-	-	-
[L1] Centro de Cableado	[A.10]	-	{3.3}	-	-	-	-	-
[L1] Centro de Cableado	[A.11]	-	{3.3}	{4.5}	{5.1}	-	-	-
[L1] Centro de Cableado	[A.12]	-	-	{2.1}	-	-	-	-
[L1] Centro de Cableado	[A.14]	-	-	{3.3}	-	-	-	-
[L1] Centro de Cableado	[A.15]	-	{3.3}	-	-	-	-	-
[L1] Centro de Cableado	[A.18]	{5.7}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.24]	{6.6}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.26]	{5.4}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.27]	{6.2}	-	-	-	-	-	-

Fuente: autor

5.7 ANÁLISIS DE SALVAGUARDAS

5.7.1 Clasificación de salvaguardas

Tabla 13. Escala Salvaguardas

CLASIFICACION SALVAGUARDAS	
Nivel	Significado
L0	Inexistente

L1	Inicial / ad hoc
L2	Reproducible, pero intuitivo
L3	Proceso definido
L4	Gestionado y medible
L5	Optimizado

Fuente: autor

5.7.2 Identificación de salvaguardas

Tabla 14. Valoración Salvaguardas

Salvaguarda	Tipo
[SW] Protección de las Aplicaciones Informáticas (SW)	L2-L4
[SW.1] Administración	L2-L3
[SW.1.1] Se dispone de un inventario de aplicaciones (SW)	L3
[SW.1.2] Se dispone de normativa relativa a las aplicaciones (SW)	L2
[SW.1.3] Se dispone de procedimientos de uso de las aplicaciones	L2
[SW.1.4] IPR: Se protegen los derechos de propiedad intelectual de las aplicaciones (SW)	L2-L3
[SW.backup] Copias de seguridad (backup) (SW)	L2-L3
[SW.SC] Se aplican perfiles de seguridad	L3-L4
[SW.op] Operación / Producción	L2-L3
[SW.op.1] Se dispone de normativa relativa al software en producción	L2
[SW.op.2] Los sistemas de producción no contienen herramientas de desarrollo	L3
[SW.op.3] {xor} Se controla la integridad del código ejecutable	L3
Tabla 14. Continuación	
[SW.op.4] El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico	L3
[SW.op.5] Aislamiento de sistemas que manejen asuntos delicados	L2-L3
[SW.op.6] Seguridad de las aplicaciones	L2-L3
[SW.op.7] Seguridad de los ficheros de datos de la aplicación	L3
[SW.op.8] Se protegen los ficheros de configuración	L3
[SW.op.9] Se protegen los ficheros del sistema	L3
[SW.op.a] Se controla la ejecución de código móvil (ej. 'applets')	L2-L3
[SW.op.b] Ejecución de programas colaborativos (ej. teleconferencia)	L3
[SW.op.c] Seguridad de los mecanismos de comunicación entre procesos	L3
[SW.op.d] Regularmente se realiza un análisis de vulnerabilidades, y se actúa en	L3

Salvaguarda	Tipo
consecuencia	
[SW.op.e] Formación del personal en configuración de aplicaciones	L2
[SW.CM] Cambios (actualizaciones y mantenimiento)	L2-L3
[SW.CM.1] Se dispone de una política	L2
[SW.CM.2] Se dispone de procedimientos para ejecutar cambios	L2
[SW.CM.3] Se hace un seguimiento permanente de actualizaciones y parches	L3
[SW.CM.4] Evaluación del impacto y riesgo residual tras el cambio	L2
[SW.CM.5] Se priorizan las actuaciones encaminadas a corregir riesgos elevados	L3
[SW.CM.6] Se mantiene en todo momento la regla de 'funcionalidad mínima'	L3
[SW.CM.7] Se mantiene en todo momento la regla de 'seguridad por defecto'	L3
[SW.CM.8] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	L3
[SW.CM.9] Se planifica el cambio de forma que minimice la interrupción del servicio	L2
[SW.CM.a] Control de versiones de toda actualización del software	L3
[SW.CM.b] Realización por personal debidamente autorizado	L3
[SW.CM.c] Se retienen copias de las versiones anteriores de software como medida de precaución para contingencias	L3
[SW.CM.d] Se retienen copias de las versiones anteriores de configuración	L3
[SW.CM.e] Se prueba previamente en un equipo que no esté en producción	L3
[SW.CM.f] Pruebas de regresión	L3
[SW.CM.g] Se registra toda actualización de SW	L2
[SW.CM.h] Documentación	L2
[SW.CM.i] Se actualizan todos los procedimientos de producción afectados	L3
[SW.CM.j] Se actualizan todos los procedimientos de recuperación afectados	L2
[SW.end] Desmantelamiento	L3
[HW] Protección de los Equipos Informáticos (HW)	L2-L4
[HW.1] Administración	L2
[HW.1.1] Se dispone de un inventario de equipos (HW)	L2
[HW.1.2] Se dispone de normativa sobre el uso correcto de los equipos	L2
Tabla 14. Continuación	
[HW.1.3] Se dispone de procedimientos de uso del equipamiento	L2
[HW.start] Puesta en producción	L3
[HW.SC] Se aplican perfiles de seguridad	L3-L4
[HW.cont] Aseguramiento de la disponibilidad	L2-L4
[HW.cont.1] Se dimensiona holgadamente y se planifica la adquisición de repuestos	L4
[HW.cont.2] El mantenimiento periódico se ajusta a las especificaciones de los fabricantes	L3
[HW.cont.3] El mantenimiento lo realiza personal debidamente autorizado	L3
[HW.cont.4] Se ejecutan regularmente las rutinas de diagnóstico	L2
[HW.cont.5] Se monitorizan fallos e incidentes	L3
[HW.cont.6] Se registran los fallos, reales o sospechados y de mantenimiento	L3

Salvaguarda	Tipo
preventivo y correctivo	
[HW.cont.7] Se hacen copias de seguridad de la configuración	L3
[HW.cont.8] Se hacen copias de seguridad de las claves de descifrado	L3
[HW.cont.9] {xor} Opciones sustitutorias	L3
[HW.cont.9.1] Equipo alternativo	L3
[HW.cont.9.2] Equipo alternativo preconfigurado con replicación de discos síncrona o asíncrona	L3
[HW.cont.9.3] Sistema redundante propio en centro alternativo	L3
[HW.cont.9.4] Contrato de prestación de servicio con el proveedor del sistema, de acuerdo a los requisitos del negocio	L3
[HW.cont.a] {xor} Alta disponibilidad	L3
[HW.cont.b] Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento	L2
[HW.5] Los medios alternativos están sujetos a las mismas garantías de protección que los habituales	L3
[HW.6] {xor} Prevención de emanaciones electromagnéticas (TEMPEST equipment)	L3
[HW.7] Instalación	L3
[HW.op] Operación	L2-L3
[HW.op.1] Proceso de autorización de recursos para el tratamiento de la información	L2
[HW.op.2] El sistema emplea diferentes tecnologías de componentes para evitar puntos únicos de fallo tecnológico	L3
[HW.op.3] Seguridad de los equipos fuera de las instalaciones	L2-L3
[HW.op.4] Formación del personal en configuración de equipos	L3
[HW.CM] Cambios (actualizaciones y mantenimiento)	L2-L3
[HW.CM.1] Se dispone de una política	L2
[HW.CM.2] Se dispone de procedimientos para ejecutar cambios	L2
[HW.CM.3] Se siguen las recomendaciones del fabricante o proveedor	L3
[HW.CM.4] Se hace un seguimiento permanente de actualizaciones	L3
Tabla 14. Continuación	
[HW.CM.5] Evaluación del impacto potencial del cambio	L2
[HW.CM.6] Se priorizan las actuaciones encaminadas a corregir riesgos elevados	L3
[HW.CM.7] Se mantiene en todo momento la regla de 'funcionalidad mínima'	L3
[HW.CM.8] Se mantiene en todo momento la regla de 'seguridad por defecto'	L3
[HW.CM.9] Se verifica que el cambio no inhabilita los mecanismos de detección, monitorización y registro	L3
[HW.CM.a] Se planifica el cambio de forma que minimice la interrupción del servicio	L2
[HW.CM.b] Realización por personal debidamente autorizado	L3
[HW.CM.c] Se retienen copias de las versiones anteriores de configuración	L3
[HW.CM.d] Se prueba previamente en un entorno que no esté en producción	L3
[HW.CM.e] Pruebas de regresión	L3
[HW.CM.f] Todos los cambios quedan registrados	L2
[HW.CM.g] Documentación	L2

Salvaguarda	Tipo
[HW.CM.h] Control de versiones de todo cambio de hw	L2
[HW.CM.i] Se actualizan todos los procedimientos de producción afectados	L3
[HW.CM.j] Se actualizan todos los procedimientos de recuperación afectados	L2
[HW.end] Desmantelamiento	L3
[HW.h] Voz, facsímil y video	L2-L3
[HW.h.1] Está prohibido establecer de conversaciones confidenciales en lugares públicos o sin adecuadas medidas de protección	L3
[HW.h.2] Está prohibido dejar mensajes confidenciales en contestadores automáticos	L3
[HW.h.3] Los usuarios están concienciados y reciben formación sobre el uso seguro de los sistemas y recursos disponibles	L2
[HW.h.4] Se controla el acceso a la memoria interna del equipo de fax	L3
[HW.h.5] Se prohíbe la programación no autorizada del equipo de fax	L3
[HW.h.6] Se previene el envío de documentos a números equivocados	L3
[AUX] Elementos Auxiliares	L2-L4
[AUX.1] Se dispone de un inventario de equipamiento auxiliar	L3
[AUX.cont] Aseguramiento de la disponibilidad	L3-L4
[AUX.cont.1] Se siguen las recomendaciones del fabricante o proveedor	L3
[AUX.cont.2] Continuidad de operaciones	L3-L4
[AUX.start] Instalación	L3
[AUX.power] Suministro eléctrico	L2-L3
[AUX.power.1] Se dimensiona el sistema considerando necesidades futuras	L3
[AUX.power.2] Instalación de acuerdo a la normativa vigente	L2
[AUX.power.3] Protección de las líneas de alimentación del sistema frente a fluctuaciones y sobrecargas	L3
[AUX.power.4] Interruptor general de la alimentación del sistema situado en la entrada de cada área	L3
Tabla 14. Continuación	
[AUX.power.5] Interruptores etiquetados y protegidos frente a activaciones accidentales	L3
[AUX.power.6] Alimentación de respaldo	L2-L3
[AUX.AC] Climatización	L3
[AUX.wires] Protección del cableado	L3-L4
[AUX.7] Se disponen medidas frente a posibles robos	L3
[AUX.8] Se prevén medidas frente a todos los problemas graves identificados en el análisis de riesgos	L3
[L] Protección de las Instalaciones	L2-L4
[L.1] Se dispone de normativa de seguridad	L2
[L.2] Se dispone de un inventario de instalaciones	L2-L3
[L.3] Entrada en servicio	L2-L3
[L.3.1] Se dispone de normativa de entrada en servicio	L2
[L.3.2] Se requiere autorización previa	L2
[L.3.3] Se han determinado las acreditaciones o certificaciones pertinentes	L3

Salvaguarda	Tipo
[L.3.4] Se requiere haber pasado las inspecciones o acreditaciones establecidas	L3
[L.3.5] Plan de Protección	L2-L3
[L.3.5.1] Se dispone de un Plan de Acondicionamiento	L3
[L.3.5.2] Se dispone de un Plan de Seguridad	L3
[L.3.5.3] Plan de Emergencia	L2-L3
[L.3.5.3.1] Plan de Evacuación	L2-L3
[L.3.5.3.2] Plan de Comunicación	L3
[L.3.5.3.3] Acceso físico a las instalaciones en caso de emergencia	L3
[L.3.5.3.4] Existe un plan de emergencia para hacer frente a la violencia	L3
[L.design] Diseño	L3
[L.design.1] El diseño atiende a las reglas y normas relevantes sobre salud y sanidad	L3
[L.design.2] Aislamiento acústico de las zonas en las que se hable de información confidencial	L3
[L.design.3] Se encuentran separadas las áreas dónde se llevan a cabo actividades peligrosas (cuartos de basura, depósitos de combustible, etc.)	L3
[L.design.4] Almacenes	L3
[L.design.4.1] los almacenes siempre están vigilados mientras permanecen abiertos	L3
[L.design.5] ventilación	L3
[L.design.5.1] Hay filtros en los conductos HVAC	L3
[L.design.5.2] Hay detectores y filtros de ántrax	L3
[L.design.5.3] Hay detectores de sustancias químicas peligrosas	L3
[L.5] {xor} Existe protección frente a emanaciones (TEMPEST facility zoning)	n.a.
[L.5.1] Zona 3: [como si] el atacante está a 500m	n.a.
[L.5.2] Zona 2: [como si] el atacante está a 100m	n.a.
Tabla 14. Continuación	
[L.5.3] Zona 1: [como si] el atacante está a menos de 20m	n.a.
[L.5.4] Zona 0: [como si] el atacante está muy cerca	n.a.
[L.6] Protección frente a desastres	L3-L4
[L.6.1] La iluminación de emergencia cubre todas las áreas necesarias para garantizar la continuidad de las misiones críticas	L3
[L.6.2] Protección frente a incendios	L3-L4
[L.6.3] Protección frente a inundaciones	L3-L4
[L.6.4] Protección frente a accidentes naturales e industriales	L3-L4
[L.6.5] Protección frente a contaminación medioambiental	L3
[L.6.6] Se ha previsto protección frente a contaminación electromagnética	L3
[L.6.7] Protección frente a explosivos	n.a.
[L.6.8] Eliminación de residuos	L3
[L.6.8.1] el sitio cuenta con un programa de recuperación y reciclaje de residuos	L3
[L.6.8.2] Se puede cerrar los contenedores de basura por la noche	L3
[L.6.9] Seguros	L3
[L.cont] Continuidad de operaciones	L3

Salvaguarda	Tipo
[L.cont.1] Se analizan las implicaciones para la continuidad del negocio	L3
[L.cont.2] Se establece un protocolo de actuación en caso de contingencia	L3
[L.cont.3] Se dispone de instalaciones alternativas	L3
[L.cont.4] El sitio cuenta con un plan para hacer frente a cualquier ataque repentino o sin previo aviso	L3
[L.8] Las instalaciones alternativas están sujetas a las mismas garantías de protección que las habituales	L2
[L.end] Desmantelamiento	L2

Fuente: autor

5.8 DETERMINACIÓN DEL IMPACTO RESIDUAL

5.8.1 Clasificación del impacto residual. El impacto residual se muestra en la siguiente escala con colores que indican su severidad.

Tabla 15. Escala Impacto Residual

ESCALA DE IMPACTO	
VALORACION	CRITERIO
[10]	Nivel 10
[9]	Nivel 9
[8]	Alto (+)
[7]	Alto
[6]	Alto (-)
[5]	Medio (+)
[4]	Medio
[3]	Medio (-)
[2]	Bajo (+)
[1]	Bajo
[0]	Despreciable

Fuente: autor

5.8.2 Identificación del impacto residual

Tabla 16. Valoración Impacto Residual

ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g1]	-	-	-	-	-	-	1
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g2]	-	-	-	-	-	-	0
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g3]	-	-	-	-	-	-	0
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g4]	-	-	-	-	-	-	0
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g5]	-	-	-	-	-	-	1
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g6]	-	-	-	-	-	-	0
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g7]	-	-	-	-	-	-	0
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g8]	-	-	-	-	-	-	1
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g9]	-	-	-	-	-	-	1
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g10]	-	-	-	-	-	-	1
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g11]	-	-	-	-	-	-	1
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g12]	-	-	-	-	-	-	0
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g13]	-	-	-	-	-	-	0
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g14]	-	-	-	-	-	-	0
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[SW1] FROZEN, [SW2] ICEBERG	[I.5]	4	-	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.8]	2	0	0	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.20]	0	0	0	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.21]	0	0	-	-	-	-	-
Tabla 16. Continuación								
[SW1] FROZEN, [SW2] ICEBERG	[A.8]	5	2	2	-	-	-	-

ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[SW1] FROZEN, [SW2] ICEBERG	[A.22]	4	2	2	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.1]	5	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.2]	4	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.*]	5	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.1]	5	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.2]	4	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.*]	5	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.3]	4	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.4]	2	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.5]	4	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.6]	5	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.7]	5	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.11]	-	-	0	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.23]	2	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.24]	4	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.25]	5	-	3	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.11]	2	0	3	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.23]	4	-	3	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.24]	5	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.25]	5	-	3	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.26]	5	-	-	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[AUX1] UPS	[N.1]	5	-	-	-	-	-	-
[AUX1] UPS	[N.2]	4	-	-	-	-	-	-
[AUX1] UPS	[N.*]	5	-	-	-	-	-	-
[AUX1] UPS	[I.1]	5	-	-	-	-	-	-
[AUX1] UPS	[I.2]	4	-	-	-	-	-	-
[AUX1] UPS	[I.*]	5	-	-	-	-	-	-
[AUX1] UPS	[I.3]	4	-	-	-	-	-	-
[AUX1] UPS	[E.23]	2	-	-	-	-	-	-
[AUX1] UPS	[A.7]	4	0	-	-	-	-	-
[AUX1] UPS	[A.23]	4	-	-	-	-	-	-
[AUX1] UPS	[A.25]	2	-	-	-	-	-	-
[AUX1] UPS	[A.26]	2	-	-	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L1] Centro de Cableado	[N.1]	5	-	-	-	-	-	-
[L1] Centro de Cableado	[N.2]	5	-	-	-	-	-	-
[L1] Centro de Cableado	[N.*]	5	-	-	-	-	-	-
Tabla 16. Continuación								
[L1] Centro de Cableado	[I.1]	5	-	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[A.22]	4	2	2	-	-	-	-

ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L1] Centro de Cableado	[I.2]	5	-	-	-	-	-	-
[L1] Centro de Cableado	[I.*]	5	-	-	-	-	-	-
[L1] Centro de Cableado	[I.3]	2	-	-	-	-	-	-
[L1] Centro de Cableado	[I.4]	2	-	-	-	-	-	-
[L1] Centro de Cableado	[I.8]	4	-	-	-	-	-	-
[L1] Centro de Cableado	[E.2]	3	1	1	-	-	-	-
[L1] Centro de Cableado	[E.9]	-	-	0	-	-	-	-
[L1] Centro de Cableado	[E.10]	-	0	-	-	-	-	-
[L1] Centro de Cableado	[E.15]	-	0	-	-	-	-	-
[L1] Centro de Cableado	[E.19]	-	-	0	-	-	-	-
[L1] Centro de Cableado	[E.24]	4	-	-	-	-	-	-
[L1] Centro de Cableado	[A.5]	-	0	2	3	-	-	-
[L1] Centro de Cableado	[A.6]	2	-	-	-	-	-	-
[L1] Centro de Cableado	[A.7]	2	0	0	-	-	-	-
[L1] Centro de Cableado	[A.9]	-	-	0	-	-	-	-
[L1] Centro de Cableado	[A.10]	-	0	-	-	-	-	-
[L1] Centro de Cableado	[A.11]	-	0	2	3	-	-	-
[L1] Centro de Cableado	[A.12]	-	-	0	-	-	-	-
[L1] Centro de Cableado	[A.14]	-	-	0	-	-	-	-
[L1] Centro de Cableado	[A.15]	-	0	-	-	-	-	-
[L1] Centro de Cableado	[A.18]	4	-	-	-	-	-	-
[L1] Centro de Cableado	[A.24]	4	-	-	-	-	-	-
[L1] Centro de Cableado	[A.26]	5	-	-	-	-	-	-
[L1] Centro de Cableado	[A.27]	5	-	-	-	-	-	-

Fuente: autor

5.9 DETERMINACIÓN DEL RIESGO RESIDUAL

5.9.1 Clasificación del riesgo residual. El riesgo residual se muestra en la siguiente escala con colores que indican su criticidad.

Tabla 17. Escala Riesgo Residual

ESCALA DE RIESGO	
VALORACION	CRITERIO
[9]	Nivel 9
[8]	Alto (+)
[7]	Alto
[6]	Alto (-)
[5]	Medio (+)
[4]	Medio
[3]	Medio (-)
[2]	Bajo (+)
[1]	Bajo
[0]	Despreciable

Fuente: autor

5.9.2 Identificación del riesgo potencial

Tabla 18. Valoración Riesgo Residual

ACTIVO	Amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g1]	-	-	-	-	-	-	{0,75}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g2]	-	-	-	-	-	-	{0,89}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g3]	-	-	-	-	-	-	{0,89}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g4]	-	-	-	-	-	-	{0,98}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g5]	-	-	-	-	-	-	{0,83}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g6]	-	-	-	-	-	-	{0,89}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g7]	-	-	-	-	-	-	{0,98}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g8]	-	-	-	-	-	-	{0,99}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g9]	-	-	-	-	-	-	{0,99}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g10]	-	-	-	-	-	-	{0,98}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g11]	-	-	-	-	-	-	{0,98}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g12]	-	-	-	-	-	-	{0,83}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g13]	-	-	-	-	-	-	{0,83}
[INF1] INFORMACIÓN DE LA EMPRESA	[PR.g14]	-	-	-	-	-	-	{0,89}
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[SW1] FROZEN, [SW2] ICEBERG	[I.5]	{2,2}	-	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.8]	{0,91}	{0,59}	{0,60}	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.20]	{0,62}	{0,75}	{0,76}	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[E.21]	{0,80}	{0,47}	-	-	-	-	-
[SW1] FROZEN, [SW2] ICEBERG	[A.8]	{2,3}	{0,94}	{0,95}	-	-	-	-
Tabla 18. Continuación								
[SW1] FROZEN, [SW2] ICEBERG	[A.22]	{2,2}	{1,0}	{1,1}	-	-	-	-

ACTIVO	Amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.1]	{1,8}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.2]	{1,3}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[N.*]	{1,8}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.1]	{2,4}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.2]	{1,9}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.*]	{2,4}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.3]	{1,2}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.4]	{0,97}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.5]	{2,1}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.6]	{2,5}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.7]	{2,4}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[I.11]	-	-	{0,50}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.23]	{0,98}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.24]	{3,0}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[E.25]	{2,6}	-	{1,5}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.11]	{0,93}	{0,70}	{1,3}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.23]	{1,8}	-	{1,2}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.24]	{2,9}	-	-	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.25]	{2,4}	-	{1,2}	-	-	-	-
[HW1] SERVIDOR 1, [HW2] SERVIDOR 2	[A.26]	{2,7}	-	-	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[AUX1] UPS	[N.1]	{1,9}	-	-	-	-	-	-
[AUX1] UPS	[N.2]	{1,3}	-	-	-	-	-	-
[AUX1] UPS	[N.*]	{1,9}	-	-	-	-	-	-
[AUX1] UPS	[I.1]	{2,5}	-	-	-	-	-	-
[AUX1] UPS	[I.2]	{2,0}	-	-	-	-	-	-
[AUX1] UPS	[I.*]	{2,5}	-	-	-	-	-	-
[AUX1] UPS	[I.3]	{1,2}	-	-	-	-	-	-
[AUX1] UPS	[E.23]	{0,98}	-	-	-	-	-	-
[AUX1] UPS	[A.7]	{2,0}	{0,38}	-	-	-	-	-
[AUX1] UPS	[A.23]	{2,1}	-	-	-	-	-	-
[AUX1] UPS	[A.25]	{0,92}	-	-	-	-	-	-
[AUX1] UPS	[A.26]	{0,99}	-	-	-	-	-	-
ACTIVO	amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L1] Centro de Cableado	[N.1]	{2,6}	-	-	-	-	-	-
[L1] Centro de Cableado	[N.2]	{2,6}	-	-	-	-	-	-
[L1] Centro de Cableado	[N.*]	{2,4}	-	-	-	-	-	-
[L1] Centro de Cableado	[I.1]	{2,6}	-	-	-	-	-	-
[L1] Centro de Cableado	[I.2]	{2,6}	-	-	-	-	-	-
Tabla 18. Continuación								
[L1] Centro de Cableado	[I.*]	{2,6}	-	-	-	-	-	-
[L1] Centro de Cableado	[I.3]	{0,96}	-	-	-	-	-	-

ACTIVO	Amenaza	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[L1] Centro de Cableado	[I.4]	{0,79}	-	-	-	-	-	-
[L1] Centro de Cableado	[I.8]	{2,1}	-	-	-	-	-	-
[L1] Centro de Cableado	[E.2]	{1,2}	{0,82}	{0,82}	-	-	-	-
[L1] Centro de Cableado	[E.9]	-	-	{0,71}	-	-	-	-
[L1] Centro de Cableado	[E.10]	-	{3.3}	-	-	-	-	-
[L1] Centro de Cableado	[E.15]	-	{1.5}	-	-	-	-	-
[L1] Centro de Cableado	[E.19]	-	-	{0,71}	-	-	-	-
[L1] Centro de Cableado	[E.24]	{2,1}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.5]	-	{0,74}	{1,0}	{1,5}	-	-	-
[L1] Centro de Cableado	[A.6]	{0,96}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.7]	{0,93}	{0,71}	{0,71}	-	-	-	-
[L1] Centro de Cableado	[A.9]	-	-	{0,71}	-	-	-	-
[L1] Centro de Cableado	[A.10]	-	{0,71}	-	-	-	-	-
[L1] Centro de Cableado	[A.11]	-	{0,71}	{0,95}	{1,3}	-	-	-
[L1] Centro de Cableado	[A.12]	-	-	{0,51}	-	-	-	-
[L1] Centro de Cableado	[A.14]	-	-	{0,74}	-	-	-	-
[L1] Centro de Cableado	[A.15]	-	{0,71}	-	-	-	-	-
[L1] Centro de Cableado	[A.18]	{1,9}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.24]	{3,0}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.26]	{1,8}	-	-	-	-	-	-
[L1] Centro de Cableado	[A.27]	{2,6}	-	-	-	-	-	-

Fuente: autor

6. RESULTADOS

Con el desarrollo de este trabajo de grado, se dio como resultado una visualización del estado actual de los activos de la institución, los riesgos a los que se encuentran expuestos, el impacto y riesgo potencial, el listado de salvaguardas y finalmente el impacto y riesgo residual.

A continuación, se detalla los resultados de acuerdo a la información previa detectada en cada fase, de la siguiente manera:

- Se listan los riesgos de mayor impacto a los que se encuentran expuestos los activos evaluados en la Universidad y su probabilidad de ocurrencia. De estos riesgos se hará la guía de buenas prácticas.
- Se muestra por medio de un mapa de calor el riesgo e impacto antes de aplicar salvaguardas y después con el fin de mostrar la eficiencia de las salvaguardas.
- Se muestran gráficas del impacto y riesgo potencial comparadas contra el impacto y riesgo residual.

6.1 FUEGO

Para el servidor 1 (HW1), el servidor 2 (HW2), el centro de cableado (L1) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por fuego es de un 50%-posible.

6.2 DAÑOS POR AGUA

Para el servidor 1 (HW1), el servidor 2 (HW2), el centro de cableado (L1) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por agua es de un 50%-posible.

6.3 DESASTRES INDUSTRIALES

Para el servidor 1 (HW1), el servidor 2 (HW2), el centro de cableado (L1) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-posible.

6.4 AVERÍA DE ORIGEN FÍSICO O LÓGICO (MAL ENSAMBLAJE O MALA FABRICACIÓN)

Para el servidor 1 (HW1), el servidor 2 (HW2), Frozen (SW1) y Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-posible.

6.5 CORTE DEL SUMINISTRO ELÉCTRICO

Para el servidor 1 (HW1) y el servidor 2 (HW2) la probabilidad de ocurrencia de un posible daño por corte del suministro eléctrico es de un 90%- probable.

6.6 CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD

Para el servidor 1 (HW1) y el servidor 2 (HW2) la probabilidad de ocurrencia de un posible daño por condiciones inadecuadas de temperatura o humedades de un 50%-posible.

6.7 FALLO DE SERVICIOS DE COMUNICACIONES

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por fallo de servicios de comunicaciones es de un 50%-probable.

6.8 ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por errores del administrador del sistema / de la seguridad es de un 50%-probable.

6.9 DIFUSIÓN DE SOFTWARE DAÑINO

Para Frozen (SW1) y Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por difusión de software dañino es de un 50%- probable.

6.10 ALTERACIÓN DE LA INFORMACIÓN

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por alteración de la información es de un 50%- probable.

6.11 FUGAS DE INFORMACIÓN

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por fugas de la información es de un 50%- probable.

6.12 VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)

Para Frozen (SW1) y Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por vulnerabilidades de los programas es de un 50%- probable.

6.13 ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)

Para Frozen (SW1) y Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por vulnerabilidades de los programas es de un 100%-muy probable.

6.14 CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS

Para el servidor 1 (HW1), el servidor 2 (HW2) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-probable.
Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

6.15 PÉRDIDA DE EQUIPOS

Para el servidor 1 (HW1), el servidor 2 (HW2) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-probable.

6.16 SUPLANTACIÓN DE LA IDENTIDAD

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

6.17 ABUSO DE PRIVILEGIOS DE ACCESO

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

6.18 ACCESO NO AUTORIZADO

Para el servidor 1 (HW1), el servidor 2 (HW2) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-probable.

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

6.19 INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

6.20 MANIPULACIÓN DE PROGRAMAS

Para Frozen (SW1) e Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por vulnerabilidades de los programas es de un 100%-muy probable.[71]

6.21 [RE-]ENCAMINAMIENTO DE MENSAJES

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

6.22 MANIPULACIÓN DEL HARDWARE

Para el servidor 1 (HW1), el servidor 2 (HW2) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-probable.

6.23 DENEGACIÓN DE SERVICIO

Para el servidor 1 (HW1), el servidor 2 (HW2) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-probable.

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

6.24 NO FACILITAR LA INFORMACIÓN EN MATERIA DE PROTECCIÓN DE DATOS O NO REDACTARLA DE FORMA ACCESIBLE Y FÁCIL DE ENTENDER

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.25 TRATAR DATOS INADECUADOS Y EXCESIVOS PARA LA FINALIDAD DEL TRATAMIENTO

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.26 CARECER DE UNA BASE JURÍDICA SOBRE LA QUE SE SUSTENTEN LOS TRATAMIENTOS REALIZADOS SOBRE LOS DATOS

[71] FROZEN Y ICEBERG. Probabilidad de ocurrencia. [En línea], [consultado el 23 de septiembre de 2019]. Disponible en: https:// www.academia.edu › Iceberg_catalogue

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.27 TRATAR DATOS PERSONALES CON UNA FINALIDAD DISTINTA PARA LA CUAL FUERON RECABADOS

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.28 NO DISPONER DE UNA ESTRUCTURA ORGANIZATIVA, PROCESOS Y RECURSOS PARA UNA ADECUADA GESTIÓN DE LA PRIVACIDAD EN LA ORGANIZACIÓN

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.29 ALMACENAR LOS DATOS POR PERIODOS SUPERIORES A LOS NECESARIOS PARA LA FINALIDAD DEL TRATAMIENTO Y A LA LEGISLACIÓN VIGENTE

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.30 REALIZAR TRANSFERENCIAS INTERNACIONALES A PAÍSES QUE NO OFREZCAN UN NIVEL DE PROTECCIÓN ADECUADO

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.31 NO TRAMITAR O DIFICULTAR EL EJERCICIO DE LOS DERECHOS DE LOS INTERESADOS

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.32. RESOLUCIÓN INDEBIDA DEL EJERCICIO DE DERECHOS DE LOS INTERESADOS EN TIEMPO, FORMATO Y FORMA

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.33 SELECCIONAR O MANTENER UNA RELACIÓN CON UN ENCARGADO DE TRATAMIENTO SIN DISPONER DE LAS GARANTÍAS ADECUADAS

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.34 CARECER DE MECANISMOS DE SUPERVISIÓN Y CONTROL SOBRE LAS MEDIDAS QUE REGULAN LA RELACIÓN CON UN ENCARGADO EL TRATAMIENTO

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.35 NO REGISTRAR LA CREACIÓN, MODIFICACIÓN O CANCELACIÓN DE LAS ACTIVIDADES DE TRATAMIENTO EFECTUADAS BAJO SU RESPONSABILIDAD

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.36 NO LLEVAR A CABO POR PARTE DEL RESPONSABLE DEL TRATAMIENTO UNA EVALUACIÓN DE IMPACTO ADECUADA EN LOS SUPUESTOS DETALLADOS POR LA NORMATIVA APLICABLE

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

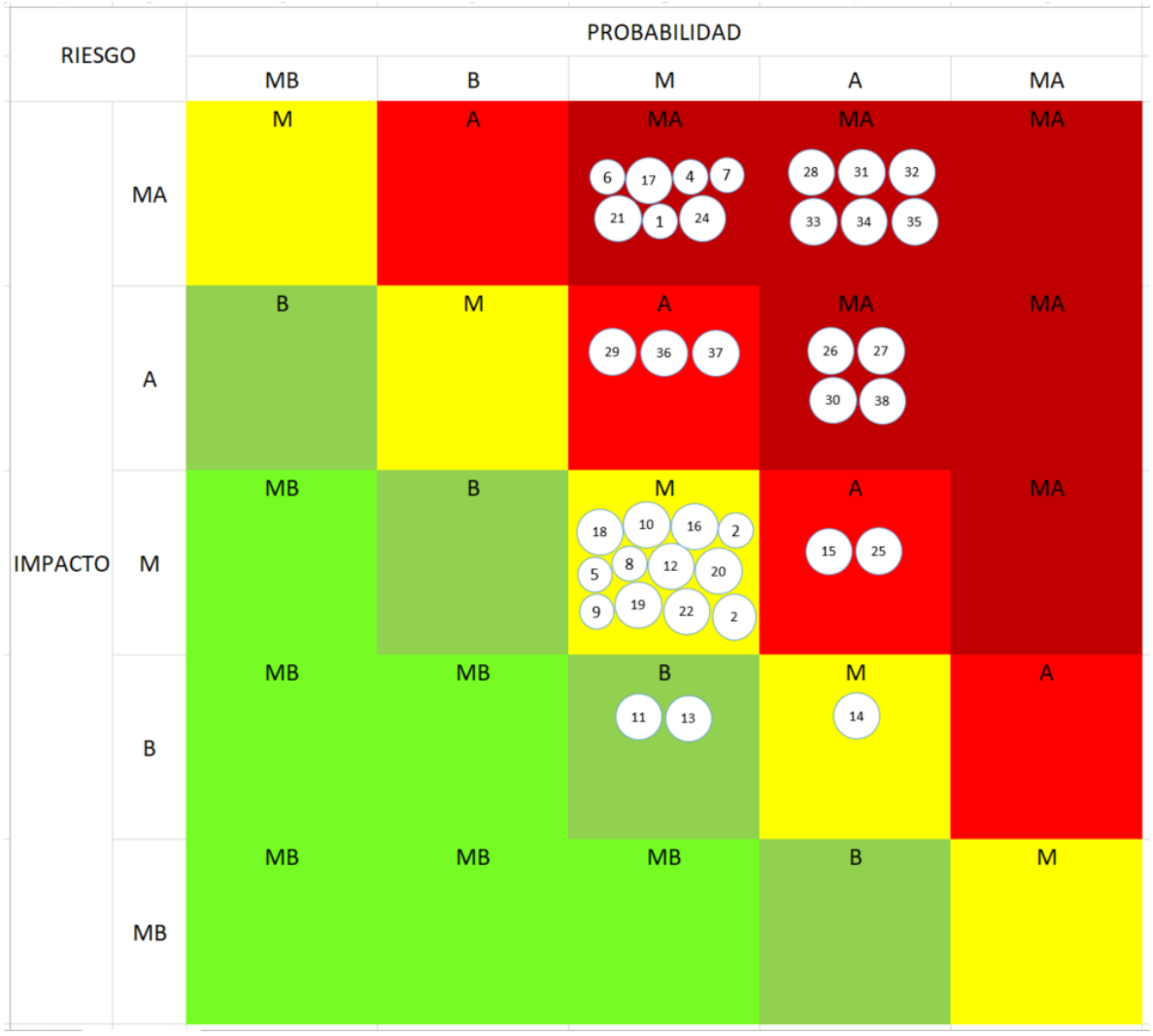
6.37 INFORMACIÓN NO ACTUALIZADA O INCORRECTA (PE. REGISTROS DUPLICADOS CON INFORMACIONES CONTRADICTORIAS O CON CAMPOS DE DATOS INCORRECTOS)

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

6.38 MAPA DE CALOR

MAPA DE CALOR SIN APLICAR CONTROLES

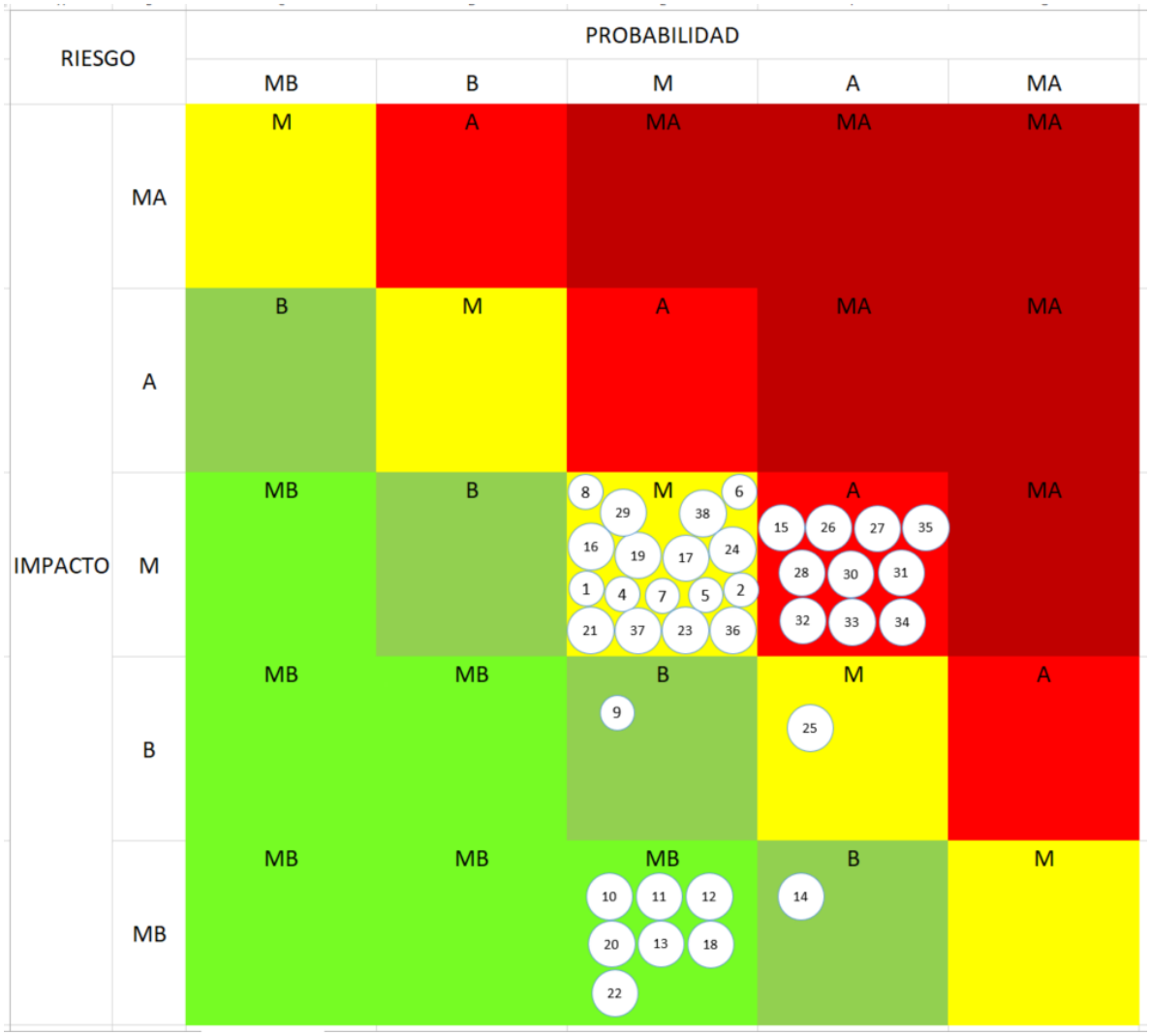
Figura 2. Mapa de Calor - riesgos antes de aplicar controles



Fuente: autor

MAPA DE CALOR APLICANDO CONTROLES

Figura 3. Mapa de Calor - riesgos después de aplicar controles

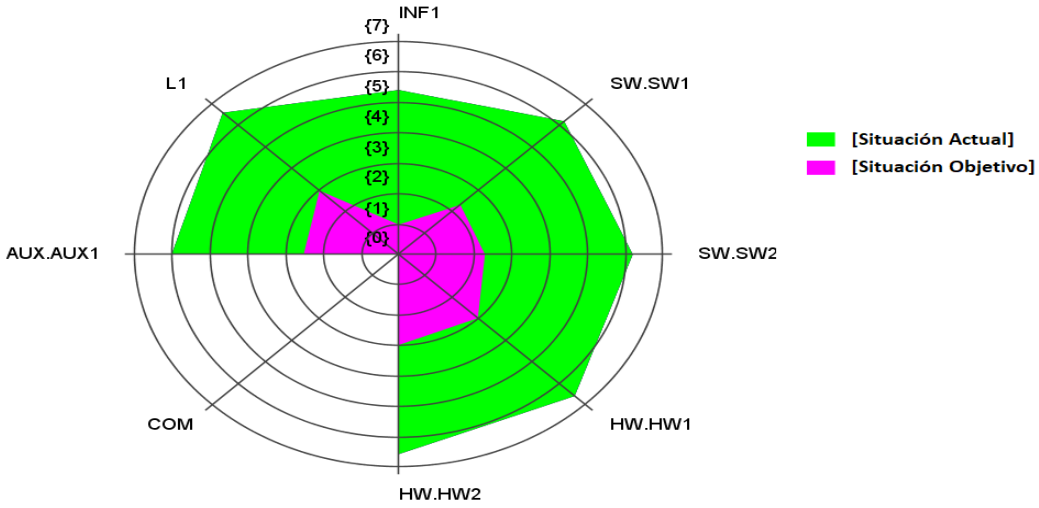


Fuente: autor

A continuación se presenta la estadística respecto al estado actual y al estado esperado del riesgo y el impacto.

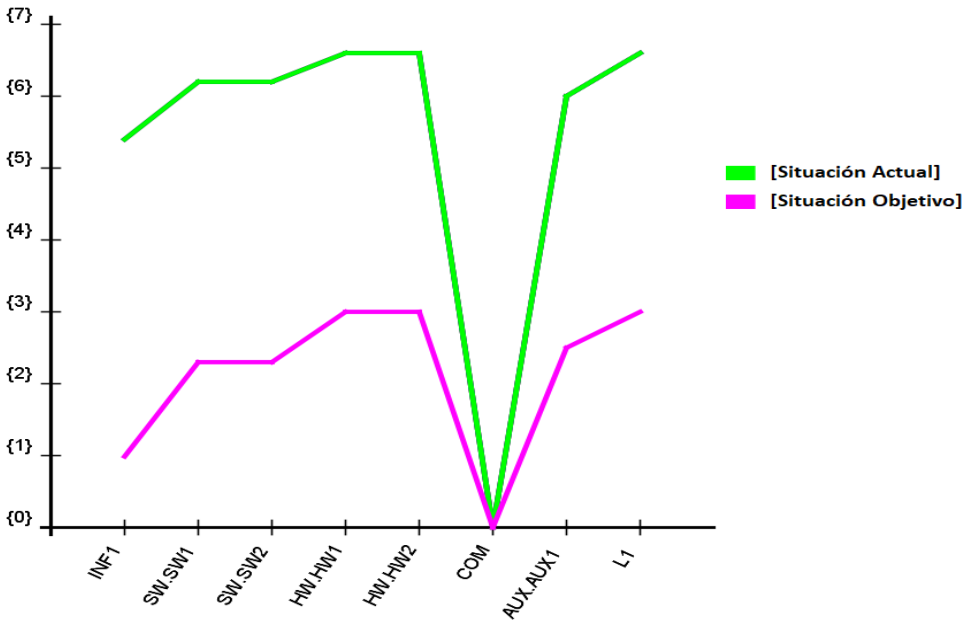
MAPA RIESGO POTENCIAL VS RIESGO RESIDUAL

Figura 4. Mapa Radial de Riesgos - Situación Actual VS Situación Objetivo



Fuente: autor

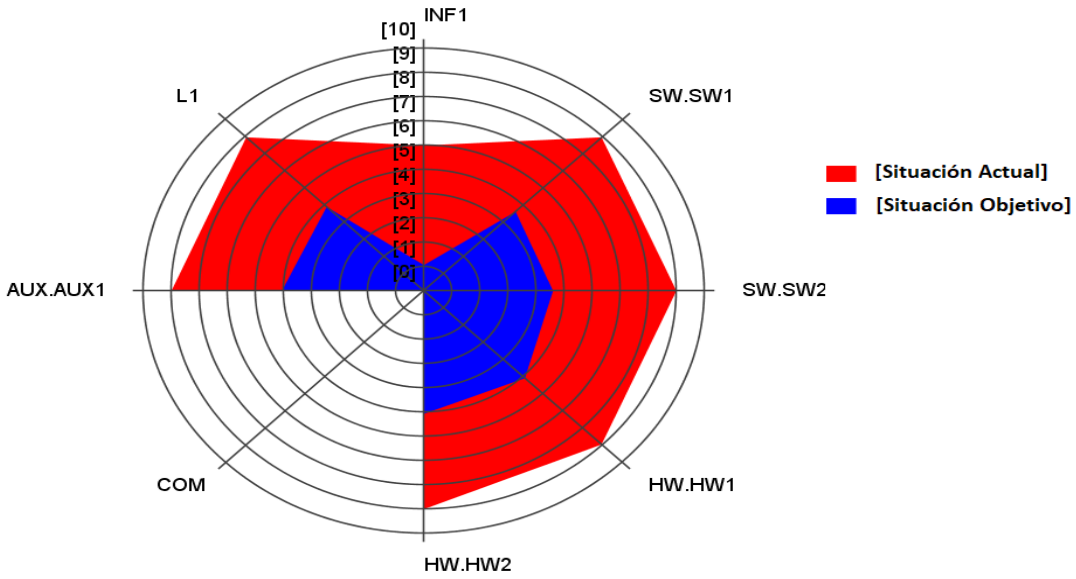
Figura 5. Mapa Lineal Riesgos Situación Actual VS Situación Objetivo



Fuente: autor

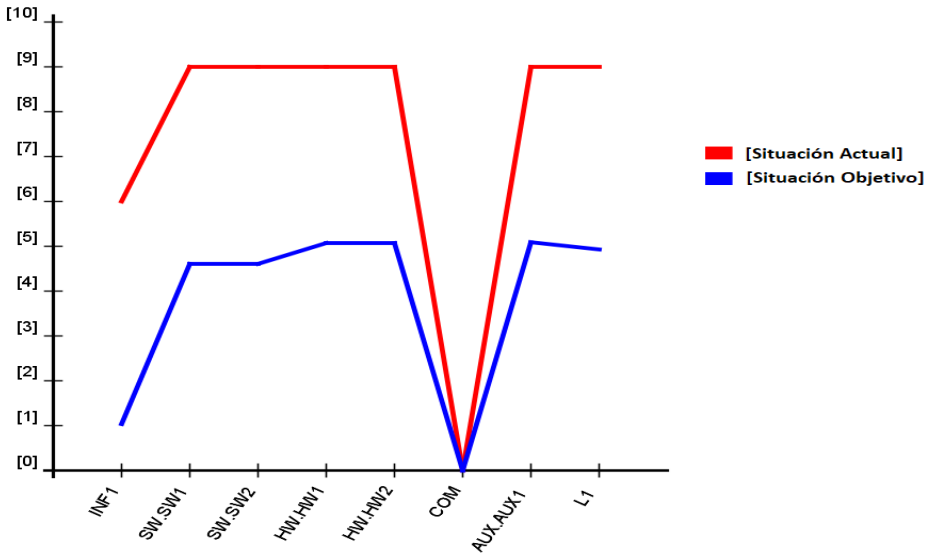
IMPACTO POTENCIAL VS IMPACTO RESIDUAL

Figura 6. Mapa Radial de Impacto - Situación Actual VS Situación Objetivo



Fuente: autor

Figura 7. Mapa Lineal Impacto Situación Actual VS Situación Objetivo



Fuente: autor

6.39 DESARROLLO DE GUIA DE BUENAS PRACTICAS

En los anexos (al final del documento) se adjunta una guía de buenas prácticas donde se plantean estrategias y recomendaciones por cada riesgo encontrado.
Esta guía muestra de forma general los vectores de ataque y riesgos encontrados y para cada uno expone su impacto y su probabilidad de ocurrencia. De igual forma para cada uno se da un detalle especifico de los controles que se deben implementar en la institución para evitar su ocurrencia y contrarrestar su ejecución. Así mismo este documento corresponde al entregable que se le proporcionara a la institución para que ellos verifiquen y hagan un chequeo frente a cada riesgo y el establecimiento de cada estrategia.

7. CONCLUSIONES

A partir del análisis realizado a los servidores de la Institución de Educación Superior se evidencia que los servidores se encuentran expuestos a una gran cantidad de riesgos (los cuales se evidencian previamente) debido a todas las amenazas tangibles e intangibles que están presentes, paralelamente a la evolución de las tecnologías de la información. De este análisis, se concluye lo siguiente:

- Existen herramientas y metodologías que permiten identificar, prevenir y en caso de materializarse, mitigar todos los riesgos encontrados. Para el caso de estudio, se utilizó la metodología Magerit, la cual propuso un esquema de estudio, donde se evidenció el estado actual de los activos, frente a riesgos informáticos y con los controles formulados la metodología brindó un estado objetivo e ideal para los activos de la Institución.

- Se mostró a la Institución el estado actual de los niveles de riesgos de los servidores y el estado objetivo e ideal con el fin de que, a partir de la verificación de las estrategias y controles aplicados, la Institución analice como disminuyen los niveles de riesgo e impacto de estos activos frente a las amenazas detectadas por medio de graficas descriptivas y mapas de calor.

- Se identificó los vectores, amenazas y riesgos potenciales que pueden afectar la operación continua de la institución, dando a conocer de cada uno la probabilidad de ocurrencia, la degradación de la vida util de los activos y el impacto potencial sobre los equipos e información propios de la institución.

- Se generó una serie de estrategias que acopladas con las salvaguardas permiten mitigar el riesgo y preparar la institución para una eventual presentación de un incidente. Así mismo estas estrategias muestran diferentes herramientas que desplegadas no solo mitigan los riesgos, sino que permiten exponer monitoreo e informes de los activos en tiempo real.

- Se entregó una guía a la institución dando a conocer todas las amenazas, vectores de ataque, riesgos encontrados y una serie de estrategias que paralelamente con los mapas de calor muestran las variaciones de los niveles de riesgo e impacto, antes y después de aplicar las salvaguardas propuestas.

8. RECOMENDACIONES

A partir del análisis y evaluación de riesgos sobre los activos presentados, se presentan las siguientes recomendaciones, con el fin de que todas se tengan en cuenta en la Universidad:

- Se sugiere realizar el análisis de las amenazas y riesgos presentados verificando que los controles formulados se estén aplicando o se apliquen en la Institución para tener un mayor control sobre los activos y las amenazas asociadas a éstos.

- Se recomienda tener en cuenta que los riesgos y los controles pueden variar de acuerdo a posibles escenarios como por ejemplo cambios sobre la infraestructura tecnológica o la implementación de nuevos proyectos lo que conlleva realizar o actualizar el análisis de riesgos realizado con el fin de mantener los niveles de seguridad independientemente los cambios en la Institución.

- Se propone crear o si se tiene, actualizar, un sistema de gestión de incidencias el cual permita gestionar cualquier amenaza o vulnerabilidad materializada y también permita recopilar las incidencias que tengan los usuarios con el fin de detectar y controlar nuevas amenazas.

- Se sugiere actualizar o realizar una política de revisión periódica de los sistemas de incidencias y al sistema de seguridad de la información con el fin de que se encuentren funcionando correctamente.

- Se recomienda incluir en los procesos de seguridad informática y la seguridad de la información de la Universidad Católica de Colombia el análisis de riesgos realizado para aumentar y mantener controlados los niveles en la seguridad de la información.

BIBLIOGRAFÍA

ÁLVAREZ MARAÑÓN, G., & PÉREZ GARCÍA, P. P. Seguridad informática para empresas y particulares. 2004. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://site.ebrary.com/ lib/unadsp/doc Detail.action? docI D=10498

BASTIDAS, E., & Guillermo, C. (2017). Identificación de vulnerabilidades de los servicios tecnológicos de la unión de cooperativas de ahorro y crédito del norte aplicando la práctica de Pentesting. . [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://repositorio.utn.edu.ec/handle/ 1234567 89/7396

COMISION DE REGULACION DE TELECOMUNICACIONES. Resolución 1732 de 17 de sep. De 2007. Colombia: Diario Oficial No. 46.756. 2007. 58 p.

CONSEJO SUPERIOR DE LA JUDICATURA. Acuerdo nº PSAA06-3334 de 2 de marzo de 2006. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://normograma.info>docs>pdf> acuerdo__csjudicatura_3334_2006

CORTE CONSTITUCIONAL. Ley 1266 de 31 de diciembre de 2008. Colombia: Diario Oficial nº 47.219. 2008. 9 p.

COSTAS SANTOS, J. Seguridad y alta disponibilidad. 2014 [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://site.ebrary.com/lib/unadsp/docDetail.action?docID=11046042

DÍAZ, F. J., HARARI, V., & VENOSA, P. Auditoría de seguridad de organizaciones, fortalezas y debilidades de la norma ISO 17799. Presentado en V Workshop de Investigadores en Ciencias de la Computación. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://hdl.handle. net/109 15/21394

DIRECCIÓN NACIONAL DEL DERECHO DE AUTOR. Decreto 1360, de 23 de junio de 1989. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://propiedadintelectual.unal.edu.co. recursos>docs>normatividad

ESCRIVÁ GASCÓ, G., ROMERO SERRANO, R. M., & RAMADA, D. J. Seguridad informática. 2013. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://site.ebrary.com/lib/unadsp/docDetail. action?docID=10820963

FROZEN Y ICEBERG. Probabilidad de ocurrencia. [En línea], [consultado el 23 de septiembre de 2019]. Disponible en: https:// www.academia.edu › Iceberg_catalogue

FUNCION PÚBLICA. Ley 962 de julio 8 de 2005. Colombia: Diario Oficial 45963, 2005. 17 p,

GALINDO, G., & MAURICIO, D. Desarrollo del sistema de gestión de seguridad de la información (sgsi) alineado con el estándar iso 27001 y sus requisitos básicos en la aplicación del ciclo phva. 11. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: https://idus.us.es/xmlui/handle/11441/45643.

GOMEZ LOPEZ & GÒMEZ LÓPEZ. Seguridad informática. 2014. Bogotá: Editorial Rama. 108 p.

JIMÉNEZ, L. de, & Elizabeth, R. (2017). Pruebas de penetración en aplicaciones web usando hackeo ético. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://www.redicces.org.sv:80/ jspui/handle/10972/3018

LEGISLACIÓN INFORMÁTICA DE COLOMBIA. Ley de Protección de datos de 1988. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: Informática Jurídica website: http://www.informatica-juridica.com/legislacion/colombia/

LEGISLACION INFORMATICA DE COLOMBIA. Proyecto de ley estatutaria No. 1266. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Decreto 1900 de 1990. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.informatica-juridica.com.>legislacion-informatica

_____. Decreto 2150 de 1995. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.informatica-juridica.com.>legislacion-informatica

_____. Ley 527 de agosto 18 de 1999. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.informatica-juridica.com.>legislacion-informatica

_____. Resolución 7652/2000, de 22 de septiembre [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Ley 35 de 2001. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Ley 679 de 3 de agosto de 2001. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Decreto 55 de febrero 15 de 2002 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Resolución 600/2002 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Resolución 20 de 2003 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Ley 890 de 7 de julio de 2004. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/ colombia/

_____. Ley 892 de 7 de julio 2004. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/ colombia/

LUJÁN MORA, S. Programación de aplicaciones web: historia, principios básicos y clientes web. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://rua.ua.es/dspace/handle/10045/16995

MAGERIT, Pilar. Metodología de análisis y gestión de riesgos de los sistemas de información. V. 3 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https:// administracióneléctronica. gob.es> pae.home>

_____. Herramientas para el análisis de riesgos. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https:// www.ccn-cert.cni.es › soluciones-seguridad › ear-pilar

MAIWALD, E., & MIGUEL, E. A. Fundamentos de seguridad de redes. México: McGraw-Hill, 2005.

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Resolución 1271 de 24 de junio de 2004. En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.mincit.gov.co.Resolucion-1271-del-24-de junio-de-2005.

PINZÓN, G., & ALFONSO, H. Pentesting al proyecto web «Quadodo Login Script» desarrollado y soportado en lenguaje PHP versión 5.5.0. 2017. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://repository.unad. edu.co/handle/10596/13378

PONCE, S., & PATRICIO, E. (2018). Análisis de los ataques a aplicaciones web SQL Injection y Cross Site Scripting y sus medidas de precaución y defensa. [En

línea], [consultado el 7 de octubre de 2019]. Disponible en: http://repositorio. utn.edu.ec/handle/123456789/7803

RAYA CABRERA & RAYA GONZALEZ. Riesgo Informático. Bogotá: Grupo Editorial Norma, 2014. 356 p.

RAZO, C. M. Auditoría en sistemas computacionales. México: Pearson Educación, 2002. 970 p.

RED NACIONAL DE FOMENTO AL TELETRABAJO. Ley 1221 de julio 16 de 2008. Diario Oficial No. 47052. 2007. 58 p.

REVISTA SEMANA. Así está Colombia en el ranking de ciberseguridad mundial. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: website: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

ROYER. 2004. Estudio comparativo entre las metodologías cramm y magerit para la gestión de riesgo de ti en las mpymes. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: revistas.uazuay.edu.ec>index-php.

RUIZ PALMERO, J., & SÁNCHEZ RODRÍGUEZ, J. El impacto del proyecto de centros TIC desde la experiencia vivida por el alumnado. 2007. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: https://idus.us.es/ xmlui/ handle/11441/45643.

SAUCEDO, A. L. H., & MIRANDA, J. M. (2016). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web. 4(1). 2016 [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://revistas cientificas.udg.mx/index.php/REC/article/view/5208

SOLARTE, F. N. S., ROSERO, E. R. E., & BENAVIDES, M. del C. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5). [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

ANEXOS

Pág.

GUIA DE BUENAS PRACTICAS - RIESGOS INFORMÁTICOS Y ESTRATEGIAS - APLICACIÓN EN SERVIDORES DE PROYECTOS ADMINISTRATIVOS DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR

JEFERSON CORTES POVEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

CONTENIDO

pág.

LISTA DE FIGURAS Pág.

LISTA DE TABLAS

INTRODUCCIÓN

La presente guía está orientada a la revisión de la seguridad informática de ciertos activos en una institución de educación superior, revisión que comprende la evaluación de riesgos desde lo físico hasta lo más intangible como lo son aplicaciones y sistemas de información.

Según un estudio realizado en Latinoamérica, Colombia se encuentra en una calificación media frente al tema de la seguridad informática. Con una evaluación realizada a 6 países, Colombia quedó en el puesto número 5, siendo el primero el peor de los 6. Esto se debe a que ha mejorado el estándar en las empresas frente a la gestión de la seguridad de la información[72].

Sin embargo, Colombia, dentro de sus políticas para la creación de pymes y corporaciones, debería exigir ciertas condiciones de seguridad informática y garantizar la implementación de SGSI, apoyando estas iniciativas con fondos del estado para las pymes y corporaciones que se encuentran en su fase de crecimiento empresarial.

Así pues, el trabajo aplicado se enfoca en realizar una evaluación de los riesgos a los que se someten los activos de una institución de educación superior para revisar qué controles pueden aplicarse frente a las amenazas y vulnerabilidades que pueden afectar la información de esta institución.

Esta evaluación se fundamentó en la metodología Magerit, metodología que comienza desde la identificación de los activos de la institución hasta todos los procesos para controlar, eliminar, compartir y aceptar el riesgo.

De esta evaluación se presentaron todos los vectores de ataques a los que se encuentran expuestos los servidores y se produjeron estrategias para el tratamiento de riesgos basándose continuamente en la metodología Magerit.

Paralelamente se generaron salvaguardas de seguridad para la revisión periódica de los servidores, salvaguardas que colaboran con la mitigación y el tratamiento de los riesgos encontrados.

[72] COMPARITECH. Which countries have the worst (and best) cybersecurity?. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: website: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

1. ANALISIS Y VALORACIÓN

1.1 ANÁLISIS DE ACTIVOS

Se realizó la identificación de los activos esenciales dentro del alcance del proyecto y se clasificaron de acuerdo al tipo de activo.

1.1.1 Tipo de activos

[INF1] INFORMACIÓN DE LA EMPRESA: Datos confidenciales de la empresa que se guardan en los servidores.

[SW] Aplicaciones

- [SW1] FROZEN: Plataforma Web para la gestión administrativa alojada en los servidores web.

- [SW2] ICEBERG: Plataforma para la gestión financiera alojada en los servidores web

[HW] Equipos

- [HW1] SERVIDOR 1: Servidor que apoya diferentes plataformas de gestión, donde se encuentra gran parte de la información de la empresa.

- [HW2] SERVIDOR 2: Servidor que apoya en servidor 1 en la temática de backups e implementación de pruebas.

[AUX] Elementos auxiliares

- [AUX1] UPS: Es un dispositivo que proporciona energía eléctrica por un tiempo limitado a todos los equipos que estén conectados a cierta red eléctrica, durante un apagón.

[L] Instalaciones

- [L1] Centro de Cableado: La zona de cableado es el lugar donde se crean las redes de **área** local.

1.2 DIMENSIONES DE SEGURIDAD

[D] Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. («Norma UNE 71504:2008», s. f.)
[I] Integridad de los datos: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. («Norma UNE 71504:2008», s. f.)
[C] Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. («Norma UNE 71504:2008», s. f.)
[A] Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. («Norma UNE 71504:2008», s. f.)
[T] Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. («Norma UNE 71504:2008», s. f.)
[V] Valor: Propiedad o característica consistente en el valor que tienen los activos para la empresa, en específico, si corresponde a patrimonio de la misma. («Norma UNE 71504:2008», s. f.)
[DP] Datos Personales: Propiedad o característica consistente en los datos confidenciales de la empresa. («Norma UNE 71504:2008», s. f.)

1.3 VALORACION DE LOS ACTIVOS

Para cada valoración se debe tener en cuenta la siguiente información:
- Criterios de valoración
- Dimensiones (Ver numeral 4.2)

Tabla 19. Escalas de valoración de activos

VALOR		CRITERIO
10	EXTREMO	Daño extremadamente grave.
9	MUY ALTO	Daño muy grave.
6-8	ALTO	Daño grave.
3-5	MEDIO	Daño importante.
1-2	BAJO	Daño menor.
0	DESPRECIABLE	Irrelevante.

Fuente: autor

Tabla 20. Valoración de activos

ACTIVOS	DIMENSIONES						
	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[INF1] INFORMACIÓN DE LA EMPRESA	9	7	7		7	9	6
[SW] Aplicaciones							
[SW1] FROZEN	7	7	7	7	7	6	[n.a]
[SW2] ICEBERG	7	7	7	7	7	6	[n.a]
[HW] Equipos							
[HW1] SERVIDOR 1	7	6	8	7	7	6	6
[HW2] SERVIDOR 2	7	6	8	7	7	6	6
[AUX] Elementos auxiliares							
[AUX1] UPS	8	6	[n.a]	[n.a]	[n.a]	6	[n.a]
[L] Instalaciones							
[L1] Centro de Cableado	7	7	7	7	[n.a]	6	[n.a]

Fuente: autor

2. IDENTIFICACIÓN DE RIESGOS

A continuación, se listan los riesgos más importantes a los que se encuentran expuestos los activos evaluados en la Universidad y su probabilidad de ocurrencia:

2.1 FUEGO

Para el servidor 1 (HW1), el servidor 2 (HW2), el centro de cableado (L1) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por fuego es de un 50%-posible.

2.2 DAÑOS POR AGUA

Para el servidor 1 (HW1), el servidor 2 (HW2), el centro de cableado (L1) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por agua es de un 50%-posible.

2.3 DESASTRES INDUSTRIALES

Para el servidor 1 (HW1), el servidor 2 (HW2), el centro de cableado (L1) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-posible.

2.4 AVERÍA DE ORIGEN FÍSICO O LÓGICO (MAL ENSAMBLAJE O MALA FABRICACIÓN)

Para el servidor 1 (HW1), el servidor 2 (HW2), Frozen (SW1) y Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-posible.

2.5 CORTE DEL SUMINISTRO ELÉCTRICO

Para el servidor 1 (HW1) y el servidor 2 (HW2) la probabilidad de ocurrencia de un posible daño por corte del suministro eléctrico es de un 90%- probable.

2.6 CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD

Para el servidor 1 (HW1) y el servidor 2 (HW2) la probabilidad de ocurrencia de un posible daño por condiciones inadecuadas de temperatura o humedades de un 50%-posible.

2.7 FALLO DE SERVICIOS DE COMUNICACIONES

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por fallo de servicios de comunicaciones es de un 50%-probable.

2.8 ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por errores del administrador del sistema / de la seguridad es de un 50%-probable.

2.9 DIFUSIÓN DE SOFTWARE DAÑINO

Para Frozen (SW1) y Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por difusión de software dañino es de un 50%- probable.

2.10 ALTERACIÓN DE LA INFORMACIÓN

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por alteración de la información es de un 50%- probable.

2.11 FUGAS DE INFORMACIÓN

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por fugas de la información es de un 50%- probable.

2.12 VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)

Para Frozen (SW1) y Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por vulnerabilidades de los programas es de un 50%- probable.

2.13 ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)

Para Frozen (SW1) y Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por vulnerabilidades de los programas es de un 100%-muy probable.

2.14 CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS

Para el servidor 1 (HW1), el servidor 2 (HW2) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-probable.
Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

2.15 PÉRDIDA DE EQUIPOS

Para el servidor 1 (HW1), el servidor 2 (HW2) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-probable.

2.16 SUPLANTACIÓN DE LA IDENTIDAD

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

2.17 INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)

Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

2.18 MANIPULACIÓN DE PROGRAMAS

Para Frozen (SW1) e Iceberg (SW2) la probabilidad de ocurrencia de un posible daño por vulnerabilidades de los programas es de un 100%-muy probable.[73]

2.19 MANIPULACIÓN DEL HARDWARE

Para el servidor 1 (HW1), el servidor 2 (HW2) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-probable.

2.20 DENEGACIÓN DE SERVICIO

Para el servidor 1 (HW1), el servidor 2 (HW2) y la UPS (AUX1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 50%-probable.
Para el centro de cableado (L1) la probabilidad de ocurrencia de un posible daño por desastres industriales es de un 100%-muy probable.

2.21 NO FACILITAR LA INFORMACIÓN EN MATERIA DE PROTECCIÓN DE DATOS O NO REDACTARLA DE FORMA ACCESIBLE Y FÁCIL DE ENTENDER

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

2.22 TRATAR DATOS INADECUADOS Y EXCESIVOS PARA LA FINALIDAD DEL TRATAMIENTO

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

2.23 CARECER DE UNA BASE JURÍDICA SOBRE LA QUE SE SUSTENTEN LOS TRATAMIENTOS REALIZADOS SOBRE LOS DATOS

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

2.24 TRATAR DATOS PERSONALES CON UNA FINALIDAD DISTINTA PARA LA CUAL FUERON RECABADOS

[73] FROZEN Y ICEBERG. Probabilidad de ocurrencia. [En línea], [consultado el 23 de septiembre de 2019]. Disponible en: https:// www.academia.edu › Iceberg_catalogue

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

2.25 NO DISPONER DE UNA ESTRUCTURA ORGANIZATIVA, PROCESOS Y RECURSOS PARA UNA ADECUADA GESTIÓN DE LA PRIVACIDAD EN LA ORGANIZACIÓN

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

2.26 ALMACENAR LOS DATOS POR PERIODOS SUPERIORES A LOS NECESARIOS PARA LA FINALIDAD DEL TRATAMIENTO Y A LA LEGISLACIÓN VIGENTE

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

2.27 REALIZAR TRANSFERENCIAS INTERNACIONALES A PAÍSES QUE NO OFREZCAN UN NIVEL DE PROTECCIÓN ADECUADO

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

2.28 SELECCIONAR O MANTENER UNA RELACIÓN CON UN ENCARGADO DE TRATAMIENTO SIN DISPONER DE LAS GARANTÍAS ADECUADAS

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

3. ESTRATEGIAS Y RECOMENDACIONES DE SEGURIDAD

A continuación, se presentan estrategias y recomendaciones para mitigar los riesgos encontrados:

3.1 FUEGO

Para este tipo de riesgo, las técnicas más comunes para evitarlo y mitigarlo es la detección oportuna, la alarma, la supresión automática y el manejo estructural del fuego. Con las tecnologías actuales contra incendio es posible detectar la presencia de un fuego y alertar a la gente de su existencia. Los sistemas de supresión automática de incendio están diseñados e instalados para controlar o extinguir fuegos no deseados, siendo los más comunes los sistemas rociadores, hidrantes, BIE's y extintores. La señalización y el alumbrado de emergencia permiten la detección de vías de evacuación y las salidas adecuadas de los lugares de trabajo.[74]

Salvaguarda Aplicadas: [L.6] Protección frente a desastres, [L.6.2] Protección frente a incendios.

3.2 DAÑOS POR AGUA

La probabilidad de ocurrencia de este riesgo es media-baja ya que el lugar donde se encuentran los activos revisados hace seguro el lugar frente a este riesgo. Así mismo las entidades distritales como el Acueducto, están en constante vigilancia y control al respecto. Sin embargo, se deben tener en cuenta las siguientes recomendaciones al respecto:

- Implementación y mantenimiento constante a los sistemas de bombeo, drenajes de aguas lluvia y rejillas de los sótanos donde drena el agua.

- Implementación y mantenimiento constante de canales y bajantes para desagüe normal, libre de objetos.

- Buenas prácticas de saneamiento en baños y cocinetas evitando arrojar basuras u objetos solidos que impidan el buen funcionamiento de estos lugares.[75]

[74] FUNDACIÓN PARA LA PREVENCIÓN DE RIESGOS LABORALES. Riesgos de incendios – Riesgos Laborales. [En línea], [consultado el 23 de septiembre de 2019]. Disponible en: https://riesgoslaborales.saludlaboral.org/portal-preventivo/riesgos-laborales/riesgos-relacionados-con-la-seguridad-en-el-trabajo/riesgos-de-incendios/

[75] INSTITUTO DISTRITAL DE GESTION DE RIESGOS Y CAMBIO CLIMATICO. Riesgo por Inundación. [En línea], [consultado el 23 de septiembre de 2019]. https://www.idiger.gov.co/rinundacion

Salvaguarda Aplicada: [L.6] Protección frente a desastres, [L.6.3] Protección frente a inundaciones.

3.3 DESASTRES INDUSTRIALES

La institución de educación superior debe tener normas y políticas que protejan los activos más importantes de la institución de desastres industriales relacionados con:

- Protección de las instalaciones frente a incendios, inundaciones y escapes de agua. Num 7.1 y 7.2

- Protección de las instalaciones frente a sobrecarga o fluctuación eléctrica.

- Mantenimientos preventivos de limpieza y reposición de componentes electromagnéticos.

- Protección de las instalaciones frente a errores humanos y de organización.

- Empleo de soportes redundantes y realización de copias de seguridad constantes.[76]

Salvaguarda Aplicada: [L.6] Protección frente a desastres, [L.6.*] Todas las salvaguardas que dependen de [L.6]. [L.cont] Continuidad de operaciones, [L.cont.*] Todas las salvaguardas que dependen de [L.cont].

3.4 AVERÍA DE ORIGEN FÍSICO O LÓGICO (MAL ENSAMBLAJE O MALA FABRICACIÓN)

La institución debe tener garantías de los equipos bajo condiciones pactadas con los proveedores frente a temas de ensamblaje y funcionalidad.
De igual forma la institución debe tener políticas de Backup y copias de seguridad en los casos donde el equipo almacene información valiosa que pueda afectar la continuidad, al igual que debe disponer de sistemas redundantes que permitan la operación continua de la institución.

Salvaguarda Aplicada: [HW.cont.9.3] Sistema redundante propio en centro alternativo, [L.cont.3] Se dispone de instalaciones alternativas.

[76] OFICINA INTERNACIONAL DEL TRABAJO GINEBRA. Prevención de accidentes industriales mayores. [En línea], [consultado el 25 de septiembre de 2019]. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112650.pdf

3.5 CORTE DEL SUMINISTRO ELÉCTRICO

Para este riesgo, se propone tres formas de proteger los equipos que funcionen con corriente eléctrica:

- **Supresor de picos:** Este elemento permite proteger los equipos que se encuentren conectados a él de elevaciones o disminuciones eléctricas. Su funcionalidad consiste en mantener el voltaje estable, independientemente si hay variaciones en la normalidad eléctrica.

- **Reguladores de voltaje:** Un regulador de voltaje protege los equipos de las constantes variaciones eléctricas manteniendo un nivel de voltaje constante y regulado.
  Cuando recibe la corriente, el regulador detecta el voltaje y lo estabiliza a un determinado rango para después pasar la corriente a los equipos conectados a él. Además de computadoras y otros equipos electrónicos, sirven también para proteger equipos industriales e instalaciones eléctricas completas.

- **No Breaks o UPS:** Estos sistemas proporcionan energía eléctrica durante un rango de tiempo limitado permitiendo guardar la información y apagar los equipos correctamente.
  De acuerdo a su uso y la cantidad de equipos a conectar existen diversos sistemas de UPSs.[77]

Salvaguarda Aplicada: [AUX.power.6] Alimentación de respaldo, [AUX.power.5] Interruptores etiquetados y protegidos frente a activaciones accidentales, [L.cont.3] Se dispone de instalaciones alternativas, [AUX.power.2] Instalación de acuerdo a la normativa vigente, [AUX.power.3] Protección de las líneas de alimentación del sistema frente a fluctuaciones y sobrecargas, [AUX.power.4] Interruptor general de la alimentación del sistema situado en la entrada de cada área.

3.6 CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD

En este caso tanto para los equipos, como para el recurso humano se debe garantizar que los espacios de trabajo tengan como mínimo:

[77] LAGE. Formas de proteger tus equipos contra descargas eléctricas. [En línea], [consultado el 25 de septiembre de 2019]. https://www.lage.com.mx/blog/3-formas-de-proteger-equipos-contra-descargas-electricas

- Una temperatura óptima debe oscilar entre los 20 y 22ºC.

- Una ventilación o renovación periódica del aire ayuda a mantener un ambiente más limpio y contribuye a incrementar el confort y bienestar durante el desarrollo de la actividad laboral.[78]

- Una iluminación de ser posible, natural. Las ventanas deberían estar en los espacios laterales, evitando que tanto el profesor como los alumnos tuvieran ventanas frente a sí. Las ventanas no deben estar situadas frente al profesor y los alumnos sino en los laterales del aula para evitar reflejos y deslumbramientos.

Salvaguarda Aplicada: [AUX.AC] Climatización, [L.3.5.1] Se dispone de un Plan de Acondicionamiento, [L.design.5] ventilación, [L.design.5. *] Todas las que dependen de [L.design.5].

3.7 FALLO DE SERVICIOS DE COMUNICACIONES

La institución debe tener garantías de los servicios de comunicaciones bajo condiciones pactadas con los proveedores frente a funcionalidad continua en los casos de internet y telefonía principalmente. Dado el caso, deben cumplirse ciertas cláusulas de funcionamiento pactadas durante el proceso de contratación frente a prestación del servicio.
Así mismo, los proveedores deben notificar los fallos y mantenimiento de los servicios oportunamente y tomar medidas que no afecten la operación continua de las empresas.

Salvaguarda Aplicada: [L.3.5] Plan de Protección, [L.3.5.3.2] Plan de Comunicaciones, [COM] Protección de las Comunicaciones, [COM.cont.a] {xor} Redundancia, [COM.cont.b] Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento

3.8 ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD

Las recomendaciones de seguridad frente a este riesgo son las siguientes:

- Utilizar usuarios con permisos de administrador diferentes a *root(linux)* o *admin(windows)* para instalar o ejecutar programas con el fin de que los

[78] PREVENCIÓN, PROTECCIÓN Y PROTOCOLOS DE EMERGENCIA. Tipos de riesgos y su prevención. [En línea], [consultado el 25 de septiembre de 2019]. https://sites.google.com/site/prevencionderiesgosyaccidentes/tipos-de-riesgos-y-su-prevencion/riesgo-temperatura-humedad-ventilacion-iluminacion-y-ruido

usuarios administradores previamente mencionados sean utilizados únicamente para procedimientos donde sea necesaria su intervención. El hecho de utilizar *root* en todo puede ocasionar una falla en todo el sistema si son robadas las credenciales.

- No ejecutar scripts de origen desconocido o software de terceros que se desconozca. Una recomendación es que al menos se verifique el contenido de dichos paquetes y su origen.[79]

- Utilizar contraseñas diferentes para cada usuario, independientemente el software o servicios que ejecute. Tratar de que dichas contraseñas tengan una seguridad fuerte y sean diferentes para todos los casos.

- Hacer mantenimiento diario de cuentas creadas, ya que cuentas no utilizadas pueden generar puertas de vulnerabilidades.

- No compartir en lo posible cuentas de administrador con otros usuarios ya que se pueden generar cambios no deseados como habilitación de puertos o ejecución de scripts desconocidos.

Salvaguarda Aplicada: [SW.SC] Se aplican perfiles de seguridad, [SW.1.3] Se dispone de procedimientos de uso de las aplicaciones.

3.9 DIFUSIÓN DE SOFTWARE DAÑINO

Para estos riesgos existen muchas técnicas para evitar su ejecución y propagación. A continuación, se listan una serie de recomendaciones que se sugieren ejecutar de forma continua:

- Mantener actualizados los sistemas operativos de los equipos con parches y actualizaciones dadas por los fabricantes. De la misma manera mantener actualizados los programas y servicios instalados.

- Generar políticas frente a permisos de acceso a links y descargas de origen sospechoso.[80]

- Tener precaución de abrir links de correos sospechosos o imágenes adjuntas, ya que pueden albergar software malicioso.

[79] REVISTA CIO PERU. Errores de seguridad que cometen los administradores de sistemas. [En línea], [consultado el 25 de septiembre de 2019]. https://cioperu.pe/articulo/19962/10-errores-de-seguridad-que-cometen-los-administradores-de/?p=3

[80] GOOGLE ADS. Protéjase del software malicioso. [En línea], [consultado el 25 de septiembre de 2019]. https://support.google.com/google-ads/answer/2375413?hl=es-419

- Evitar dar permisos a los navegadores de paginas que pidan descargar software o que abran ventanas emergentes.

- Uso de software antivirus actualizado, con licencias al día, realizando contantemente análisis de virus. Así mismo a nivel de red, incorporar firewall, zonas delimitadas, proxys inversos, entre otros.

Salvaguarda Aplicada: [SW] Protección de las Aplicaciones Informáticas (SW), [SW.backup] Copias de seguridad (backup) (SW), [HW.PCD.a.7] Se instala software antivirus y se mantiene actualizado

3.10 ALTERACIÓN DE LA INFORMACIÓN

Para este riesgo debe disponerse de sistemas de revisión y validación de transacciones, debido a que hay una completa perdida de la integridad de la información. (Revisiones por Software, Repositorios, versiones de la información, etc.).

Salvaguarda Aplicada: [SW] Protección de las Aplicaciones Informáticas (SW), [SW.backup] Copias de seguridad (backup) (SW), [COM.I] {xor} Protección de la integridad de los datos intercambiados, [COM.i.4] Protección de la integridad de los datos, [D.I] Protección de la integridad

3.11 FUGAS DE INFORMACIÓN

Este riesgo es bastante variable ya que los escenarios donde se da, pueden ser internos o externos y se pierde toda la Confidencialidad de la Información. Las estrategias que se implementan y se recomiendan son las siguientes:

- **Implementación de sistemas DLP.** Un sistema DLP (Data Loss Prevention) son soluciones que permite explorar todo el contenido que pasa por todos los discos, equipos, puertos y protocolos de la empresa. Hay varias alternativas dependiendo los equipos o información que se deseen monitorear.[81]

- **Implementación de soluciones CMF.** Las soluciones CMF (Content Monitoring and Filtering) comprenden dispositivos y software para

[a]AUDEA CIBERSEGURIDAD. Fuga de Información ¿Qué es y cómo se puede prevenir?. [En línea], [consultado el 30 de septiembre de 2019]. https://www.audea.com/fuga-de-informacion-que-es-y-como-se-puede-prevenir/

monitorear, filtrar, censurar e impedir el acceso a contenido web restringido, considerado ofensivo o inapropiado.[82]

- **Implementación de sistemas IPC.** Las empresas tienen la necesidad de proteger la información confidencial y a la vez de compartir esa misma información entre los empleados apropiados dentro y fuera de la red corporativa. Los sistemas IPC brindan la capacidad en las instalaciones para crear y consumir contenido protegido, como correo electrónico y documentos.[83]

Todas estas herramientas pueden prevenir acontecimientos inesperados, pero deben ser minuciosamente configuradas, para lo cual se requiere previamente conocer el valor de la información y los activos de la empresa.
Salvaguarda Aplicada: [D.5] Protección de la confidencialidad, [D.C] Cifrado de la información, [D.5.2] Protección frente a minería de datos, [D.C.2] Se dispone de procedimientos relativos al cifrado de información

3.12 VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)

En los casos que se detecte defectos de software, bien sea de su programación, descuidos de fabricación, diseño, flujo o backdoors, la institución debe establecer políticas de garantías con los proveedores sobre dichos temas.
Los proveedores deben suministrar parches de actualizaciones sobre el software vendido o nuevas versiones de los programas y los servicios.
Así mismo, se debe garantizar que las vulnerabilidades de los programas no son por cuestiones de configuraciones erróneas o desconocimiento de uso de los mismos. Si se presenta este caso, los proveedores deben garantizar una capacitación mínima sobre el uso, la seguridad y los permisos que debe poseer el software en tiempo de ejecución.[84]

Salvaguarda Aplicada: [NEW.HW.b] Entorno de pruebas, [V.2] Se han previsto mecanismos para estar informados de vulnerabilidades, [NEW.1.5] Las implicaciones para la seguridad de la información se abordan y revisan

[82] TRUST RADIUS. Web Content Filtering Solutions. [En línea], [consultado el 30 de septiembre de 2019]. https://www.trustradius.com/web-content-filtering

[83] MICROSOFT. Information Protection and Control (IPC) in Microsoft Exchange Online with AD RMS whitepaper. [En línea], [consultado el 30 de septiembre de 2019]. https://www.microsoft.com/en-us/download/details.aspx?id=30139

[84] GOBIERNO DE ESPAÑA. Vulnerabilidades de un sistema informático. [En línea], [consultado el 02 de octubre de 2019]. http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

regularmente en todos los proyectos, [S.voip.5.4] Se revisan regularmente las vulnerabilidades de los algoritmos

3.13 ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)

La institución debe garantizar un ambiente de pruebas y un ambiente de producción para generar pruebas de actualizaciones o mantenimiento de software y validar que su funcionalidad sea la misma o mejor que la inicial.
Así mismo los ambientes de pruebas, al igual que producción, debe tener la misma configuración con sistemas de Firewall, DMZ y proxys inversos con el fin de que las actualizaciones o el mantenimiento estén alineados con los parámetros de seguridad definidos por la institución.

Salvaguardas aplicadas: [SW.CM] Cambios (actualizaciones y mantenimiento), [SW.CM.2] Se dispone de procedimientos para ejecutar cambios, [SW.CM.3] Se hace un seguimiento permanente de actualizaciones y parches, [SW.CM.4] Evaluación del impacto y riesgo residual tras el cambio, [SW.CM.a] Control de versiones de toda actualización del software.

3.14 CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS

Para este riesgo es importante la implementación de sistemas de monitorización de recursos que notifiquen constantemente los procesos que consumen más recursos y la cantidad de recursos consumidos. Para este riesgo se disponen de varios sistemas, algunos de código abierto, otros licenciados. A continuación, se listan los más comunes, a pesar que el mercado dispone de una gran variedad [85] de acuerdo a la necesidad de la institución:

- Acronis Monitoring Service
- New Relic
- LogicMonitor
- Nagios
- Icinga
- SolarWinds
- Paessler

Salvaguardas aplicadas: [COM.cont.4] Se monitorizan enlaces y dispositivos de red, [COM.op.2.1] Se monitorizan los servicios de red, [IP.1.3] Se realiza una monitorización continua de las conexiones autorizadas, [IP.3.3] Proxy

[85] ACRONIS. Herramientas para monitorizar aplicaciones y servidores. [En línea], [consultado el 02 de octubre de 2019]. https://www.acronis.com/es-es/articles/monitoring-tools/

(monitorización de aplicaciones), [PDS.www.2] Herramienta de monitorización del tráfico, [IR.2.8] Actuación frente a alarmas de los sistemas de monitorización de integridad de los ficheros.

3.15 PÉRDIDA DE EQUIPOS

Para este riesgo se deben implementar las siguientes acciones:

- **Alarmas antirrobo.** Estos sistemas brindan una mayor seguridad para computadores, portátiles, monitores y servidores con el fin de brindar seguridad mecánica sólida combinada con una alarma activada por códigos de seguridad.

- **Sistemas de anclaje de los equipos.** Los anclajes están diseñados para ser fijados a una estructura y según la necesidad pueden ser fijos o temporales. Estos anclajes fijan equipos dando protección contra robos y caídas en los edificios, estructuras, o áreas a las que se accede con cierta frecuencia.

- **Técnicas de criptografía.** Técnicas de cifrado hay varias, cada una va desde los tipos de algoritmos (AES, RSA) a usar como la forma de encriptar la información que puede ser de forma simétrica o asimétrica. El uso y configuración de estas técnicas dependen de la necesidad de la institución y el presupuesto disponible para este tema.[86]

Salvaguardas aplicadas: [HW.1.1] Se dispone de un inventario de equipos, [HW.op.3] Seguridad de los equipos fuera de las instalaciones, [HW.PCD.a.1] Se han determinado las medidas para la protección física del dispositivo, [HW.PCD.a.2] Se instalan detectores de violación, [HW.PCD.a.3] Se han establecido los requisitos sobre control de acceso, [HW.PCD.a.4] Se utiliza un sistema de defensa perimetral (cortafuegos), [HW.PCD.a.5] Se han establecido los requisitos de cifrado, [HW.PCD.a.6] Se han establecido los requisitos sobre copias de seguridad (backups).

3.16 SUPLANTACIÓN DE LA IDENTIDAD

Este caso se da de forma constante en las empresas, ya que los directivos proporcionan claves y usuarios a sus empleados para colaboración de trabajo, sin tener en cuenta los riesgos de robo de datos o acceso a información privada a

[86] NEXTVISION CIBERSEGURIDAD. Encriptación de datos para empresas. [En línea], [consultado el 02 de octubre de 2019]. https://nextvision.com/2017/08/24/todo-sobre-encriptacion-de-datos-para-empresas/

personal no autorizado. Para este riesgo se deben implementar sistemas de autenticación fuerte con algunos de los siguientes elementos.

- **Sistemas de autenticación con tokens.** Estos sistemas incluyen la verificación por medio de Códigos o Tokens que se encuentran en los celulares o correos.
- **Sistemas de autenticación con OTP (One Time Password).** Estos sistemas incluyen un inicio de sesión inicial y luego envían un código a un correo o celular que deben ingresar después de la autenticación.[87]

- **Sistemas de autenticación con medidas biométricas.** Estos sistemas solicitan la autenticación básica y adicional solicita métodos de ingreso por huella digital, detección de rostro o detección de retina.

Salvaguardas aplicadas: [IA.4] Gestión de la identificación y autenticación de usuario, [IA.4.a] Las cuentas se suspenden al ser comprometidas o existir sospecha de ello, [IA.4.3] Se comprueba la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticador, [S.2.a.4] Implantación de mecanismos de autenticación. [COM.aut.4.5] 2 factores: contraseña de un solo uso (OTP) con token.

3.17 INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)

El riesgo asociado en este caso es el análisis de tráfico. Para evitar y contrarrestar este riesgo es necesario implementar las siguientes recomendaciones:

- **Aleatorización de las rutas de comunicaciones.** Despliegue de circuitos de conmutación de paquetes por la técnica de Datagrama, la cual envía paquetes en orden diferente al original y por diferentes canales de forma independiente.[88]

- **Encapsulamiento de protocolos.** Cuando los datos llegan a la capa de transporte, los protocolos de la capa inician el proceso de encapsulado de datos. La capa de transporte encapsula los datos de aplicación en unidades de datos de protocolo de transporte. El protocolo de capa de transporte

[87] SECUTATIS CIBERSEGURIDAD. Autenticación fuerte. [En línea], [consultado el 06 de octubre de 2019]. http://www.secutatis.com/autenticacion-fuerte/

[88] PADILLA, JHON JAIRO. Enrutamiento de paquetes. [En línea], [consultado el 06 de octubre de 2019]. http://jpadilla.docentes.upbbga.edu.co/Network_routing/1-Enrutamiento%20en%20redes%20de%20paquetes.pdf

crea un flujo virtual de datos entre la aplicación de envío y la de recepción, que se identifica con un número de puerto de transporte.[89]

- **Empleo de técnicas de criptografía.** Como se comentó anteriormente, la aplicación de cifrado de los mensajes, permite que no sean visualizados por agentes externos y siguen conservando su confidencialidad.

Salvaguardas aplicadas: [COM.wifi.7] Se aplican restricciones al protocolo SNMP en redes Wireless, [COM.wifi.5] Se desactivan los puertos y servicios no usados, [SW.op.c] Seguridad de los mecanismos de comunicación entre procesos, [COM.C] Protección criptográfica de la confidencialidad de los datos intercambiados.

3.18 MANIPULACIÓN DE PROGRAMAS

Este riesgo es común donde el software y plataformas tengan backdoors donde terceros puedan ingresar a alterar, robar o dañar información.
Para este riesgo se recomienda:

- Tener un repositorio con la última versión de los programas de modo que pueda reestablecerse un programa afectado a un punto inicial.

- Tener copias de las configuraciones de los programas y copias de seguridad de los datos.

- Aplicación de parches de actualizaciones de incluyan seguridad frente a manipulación de terceros.

Salvaguardas aplicadas: [SW.1.1] Se dispone de un inventario de aplicaciones (SW), [SW.backup] Copias de seguridad (backup) (SW), [SW.CM.3] Se hace un seguimiento permanente de actualizaciones y parches.

3.19 MANIPULACIÓN DEL HARDWARE

Este riesgo se ejecuta debido a que gente externa tiene acceso a los lugares del hardware o los dispositivos no tienen controles de acceso a sus elementos y periféricos. Para este caso se recomienda:

- Sistemas de control de acceso a los dispositivos.
- Inventario de Hardware y componentes.

[89] ORACLE. Encapsulado de datos y la pila de protocolo TCP/IP. [En línea], [consultado el 06 de octubre de 2019]. https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0s7/index.html

- Medidas de protección física a todos los dispositivos. Guayas, anclajes, alarmas.
- Sistemas detectores de violación de acceso.

Salvaguardas aplicadas: [HW.cont.b] Se establece un tiempo máximo para que los equipos alternativos entren en funcionamiento, [HW.CM.h] Control de versiones de todo cambio de hw, [HW.PCD.a.1] Se han determinado las medidas para la protección física del dispositivo, [HW.PCD.a.2] Se instalan detectores de violación, [HW.PCD.a.3] Se han establecido los requisitos sobre control de acceso

3.20 DENEGACIÓN DE SERVICIO

Este riesgo afecta principalmente a los sistemas ya que para la operación y agota los recursos.
Para este riesgo es importante la implementación de sistemas de monitorización de recursos que notifiquen constantemente los procesos que consumen más recursos y la cantidad de recursos consumidos. Para este riesgo se disponen de varios sistemas, algunos de código abierto, otros licenciados.

Para este riesgo se recomienda:

- **Penalización a solicitudes recurrentes.** Se limitan el numero de conexiones concurrentes al servidor y se bloquean las IPs con mayor trafico al mismo.

- **Monitorización de recursos disponibles y alarma.** Se pueden utilizar los mismos que se listaron en el riesgo “Caída por Agotamiento de Recursos. ”

Salvaguardas aplicadas: [COM.cont.4] Se monitorizan enlaces y dispositivos de red, [COM.op.2.1] Se monitorizan los servicios de red, [IP.1.3] Se realiza una monitorización continua de las conexiones autorizadas, [IP.3.3] Proxy (monitorización de aplicaciones), [PDS.www.2] Herramienta de monitorización del tráfico, [IR.2.8] Actuación frente a alarmas de los sistemas de monitorización de integridad de los ficheros

3.21 NO FACILITAR LA INFORMACIÓN EN MATERIA DE PROTECCIÓN DE DATOS O NO REDACTARLA DE FORMA ACCESIBLE Y FÁCIL DE ENTENDER

Para esta amenaza es importante el uso de mecanismos de cifrado, manejo de llaves criptográficas, fechado electrónico, y firmas electrónicas para los casos que se use la información por medios digitales. En los casos que se utilice de forma física debe disponerse de mecanismos de acceso y clasificación de la misma.

Salvaguardas aplicadas: [D.5] Protección de la confidencialidad, [D.C] Cifrado de la información, [D.C.1] Se dispone de normativa relativa al uso de cifrado, [D.C.2] Se dispone de procedimientos relativos al cifrado de información, [D.C.4] Mecanismo de cifrado, [D.5.2] Protección frente a minería de datos, [D.5.3] Limpieza de documentos publicados, [D.5.4] Marcado de la información.

3.22 TRATAR DATOS INADECUADOS Y EXCESIVOS PARA LA FINALIDAD DEL TRATAMIENTO

Frente a este riesgo siempre se implementan políticas y normativas de tratamiento de datos las cuales tienen un cumplimiento por parte de la institución que genera la captura de dichos datos como los usuarios que los proporcionan. Dado el caso de un incumplimiento por alguna de las partes se hacen cumplir clausulas y penalizaciones pactadas según la normatividad vigente.

[PS.5.4.3] Compromiso escrito de cumplimiento de la política y la normativa correspondiente, [PDS.TW.5] Se verifica regularmente que se cumple la política.

3.23 CARECER DE UNA BASE JURÍDICA SOBRE LA QUE SE SUSTENTEN LOS TRATAMIENTOS REALIZADOS SOBRE LOS DATOS

Las empresas y por supuesto las instituciones deben estar certificadas con las normatividades vigentes frente al tratamiento de datos. Así mismo, desde el lado de la seguridad de la información existen políticas y normas de tratamiento de datos que incluyen acuerdos de confidencialidad y permisos de autorización de usabilidad.

Salvaguardas aplicadas: [S.3.2.1] Se define la política aplicable sobre seguridad de la información, [HW.op.1] Proceso de autorización de recursos para el tratamiento de la información, [D.2] Normativa, [G.5.2] Política de Seguridad de la Organización, [G.5.3] Normas de seguridad

3.24 TRATAR DATOS PERSONALES CON UNA FINALIDAD DISTINTA PARA LA CUAL FUERON RECABADOS

Las instituciones deben garantizar que se cumplan las políticas de tratamiento de datos y los acuerdos de confidencialidad inmersos. Sin embargo, si se utilizan para otras finalidades que no están dentro de los acuerdos de confidencialidad, la institución se expone a penalizaciones legales por incumplimiento de políticas de tratamiento de datos.

Salvaguardas aplicadas: [S.3.2.6] Se contempla la protección de la información de carácter personal, [S.3.2.1] Se define la política aplicable sobre seguridad de la información, [PS.5.4.4] Acuerdos de confidencialidad, [IR.2.5] Actuación frente a violaciones de la confidencialidad, [PS.5.4.3] Compromiso escrito de cumplimiento de la política y la normativa correspondiente

3.25 NO DISPONER DE UNA ESTRUCTURA ORGANIZATIVA, PROCESOS Y RECURSOS PARA UNA ADECUADA GESTIÓN DE LA PRIVACIDAD EN LA ORGANIZACIÓN

La institución debe garantizar que cumple con los requisitos mínimos de seguridad de la información como lo son políticas, estructuras organizativas, procesos, documentación, comités, infraestructura TI, etc., que certifiquen la confidencialidad, integridad y disponibilidad de la información.

Salvaguardas aplicadas: [G.5] Documentación organizativa (normas y procedimientos), [G.1.1] Comité de seguridad de la información, [G.1.3] Se han identificado los roles y funciones requeridas, [G.1.4] Asignación de responsabilidades para la seguridad de la información, [G.1.5] Se dispone de asesoramiento especializado en seguridad, [RM.3] Se dispone de procedimientos para llevar a cabo las tareas de análisis y gestión de riesgos

3.26 ALMACENAR LOS DATOS POR PERIODOS SUPERIORES A LOS NECESARIOS PARA LA FINALIDAD DEL TRATAMIENTO Y A LA LEGISLACIÓN VIGENTE

La institución debe acogerse a las políticas vigentes de tratamiento de datos, lo que incluye su almacenamiento. Así pues, la institución debe poseer normatividad frente a retención, almacenamiento, tratamiento y eliminación de registros y estar en constante revisión del cumplimiento de dichas normas.

[PS.5.4.3] Compromiso escrito de cumplimiento de la política y la normativa correspondiente, [PDS.TW.5] Se verifica regularmente que se cumple la política, [G.9.5] Se dispone de guías sobre retención, almacenamiento, tratamiento y eliminación de los registros, [S.dir.4] Se asegura la integridad de los datos almacenados.

3.27 REALIZAR TRANSFERENCIAS INTERNACIONALES A PAÍSES QUE NO OFREZCAN UN NIVEL DE PROTECCIÓN ADECUADO

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

Salvaguardas aplicadas: [D.2.2] IPR: Se protegen los derechos de propiedad intelectual de la información, [E.1] Acuerdos para intercambio de información y software, [PS.5.4.3] Compromiso escrito de cumplimiento de la política y la normativa correspondiente.

3.28 SELECCIONAR O MANTENER UNA RELACIÓN CON UN ENCARGADO DE TRATAMIENTO SIN DISPONER DE LAS GARANTÍAS ADECUADAS

Para la información de la empresa (INF1) la probabilidad de ocurrencia por esta amenaza es de un 50%-probable.

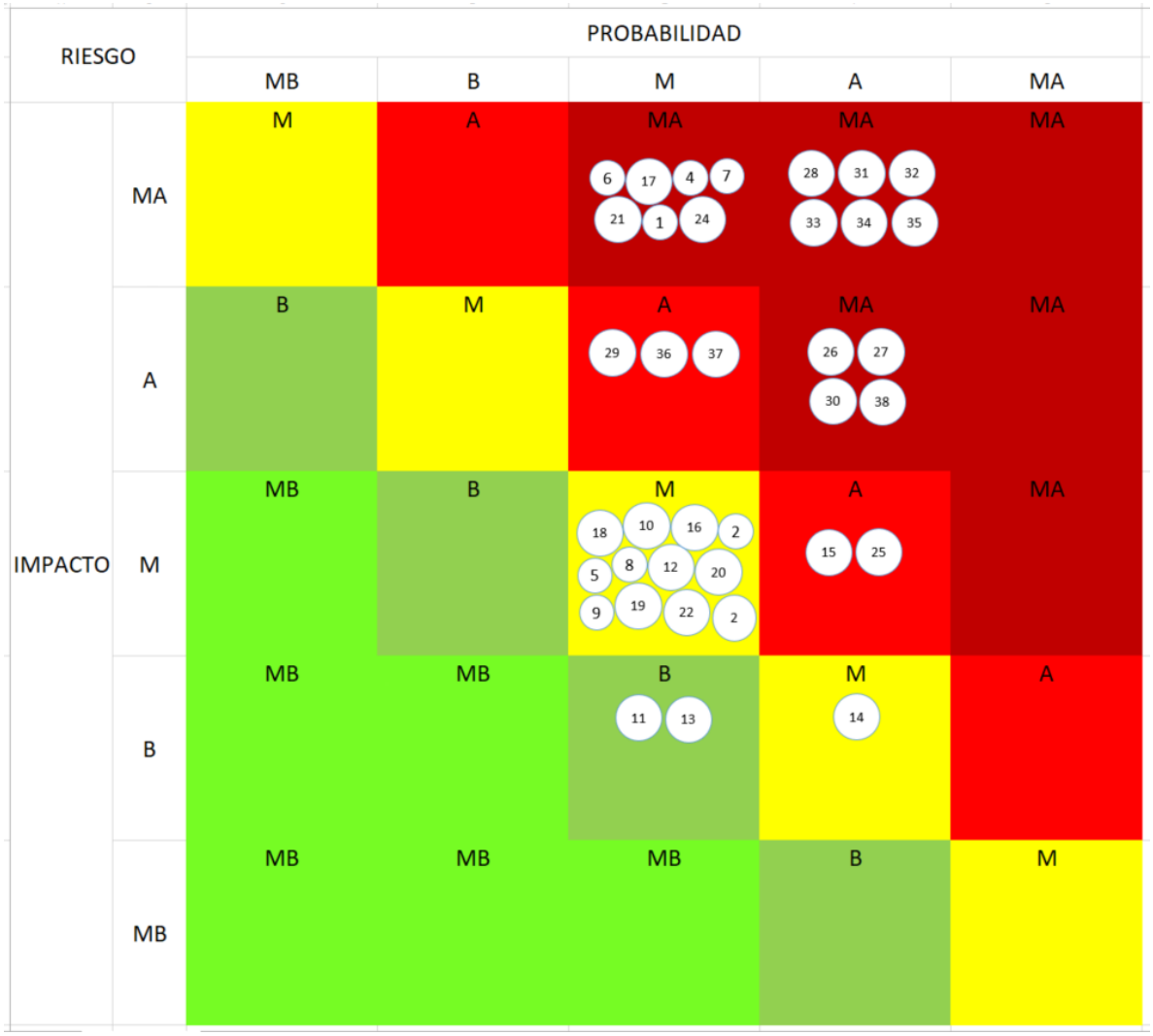
.

Salvaguardas aplicadas: [MP.4.1] Se requiere autorización previa para sacar soportes de las instalaciones, [MP.4.3] Registro de entradas y salidas, [MP.IC.1] Se dispone de normativa relativa a la protección criptográfica de los contenidos.

4. MAPA DE CALOR

4.1. MAPA DE CALOR SIN APLICAR CONTROLES

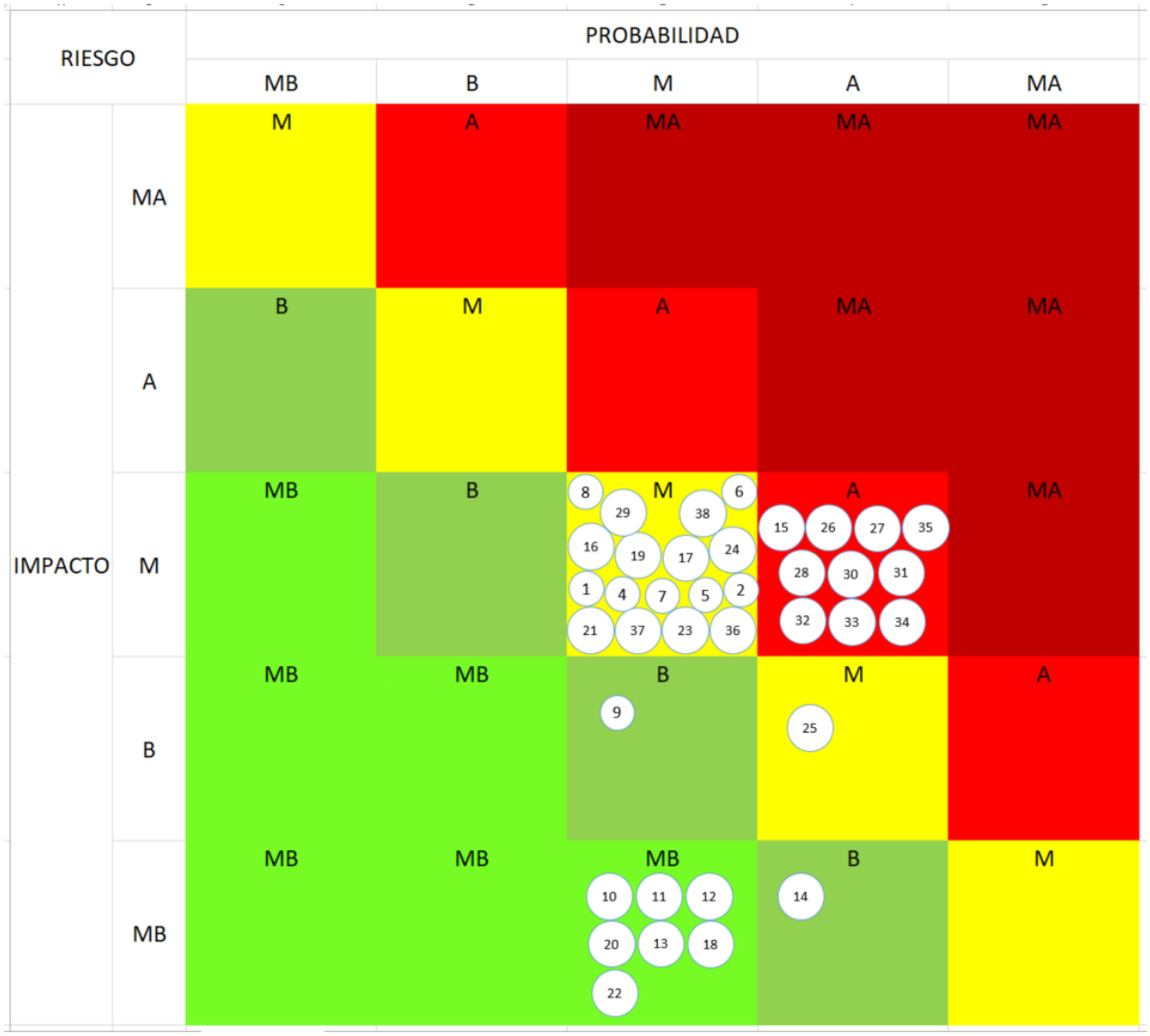
Figura 8. Mapa de Calor - riesgos antes de aplicar controles



Fuente: autor

4.2. MAPA DE CALOR APLICANDO CONTROLES

Figura 9. Mapa de Calor - riesgos después de aplicar controles

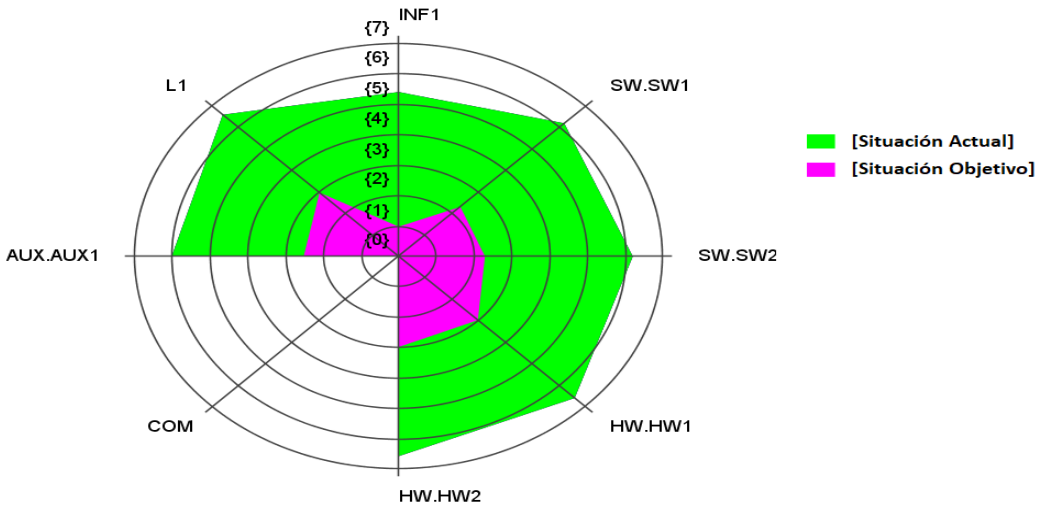


Fuente: autor

A continuación se presenta la estadística respecto al estado actual y al estado esperado del riesgo y el impacto.

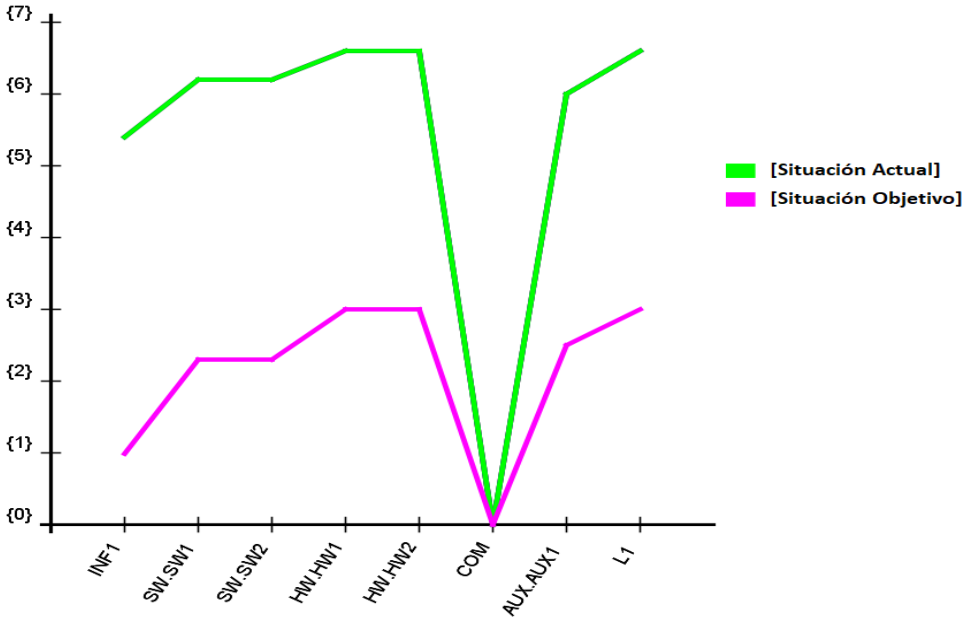
4.3. MAPA DE RIESGO POTENCIAL VS RIESGO RESIDUAL

Figura 10. Mapa Radial de Riesgos - Situación Actual VS Situación Objetivo



Fuente: autor

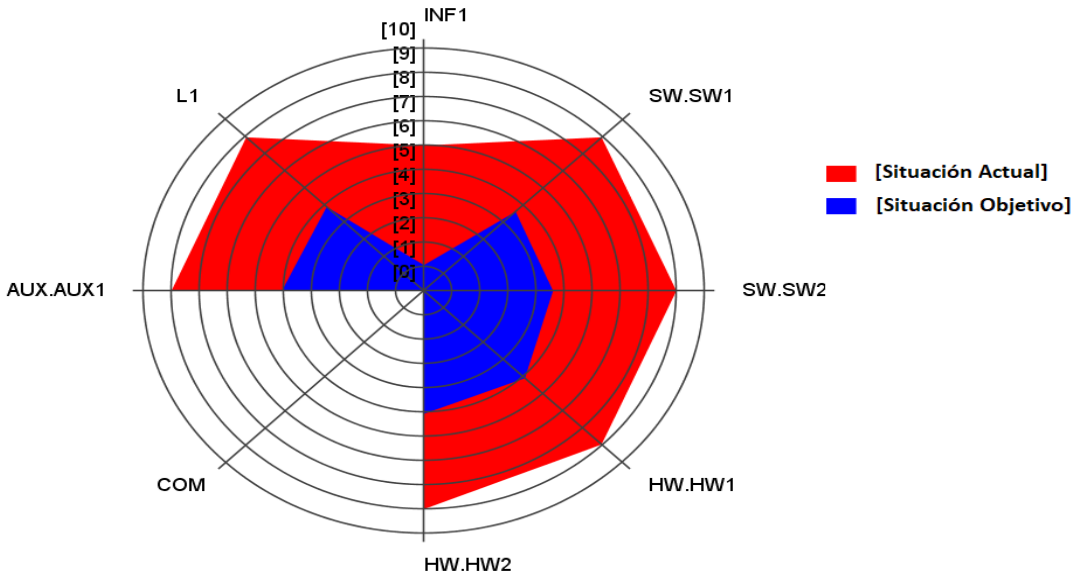
Figura 11. Mapa Lineal Riesgos Situación Actual VS Situación Objetivo



Fuente: autor

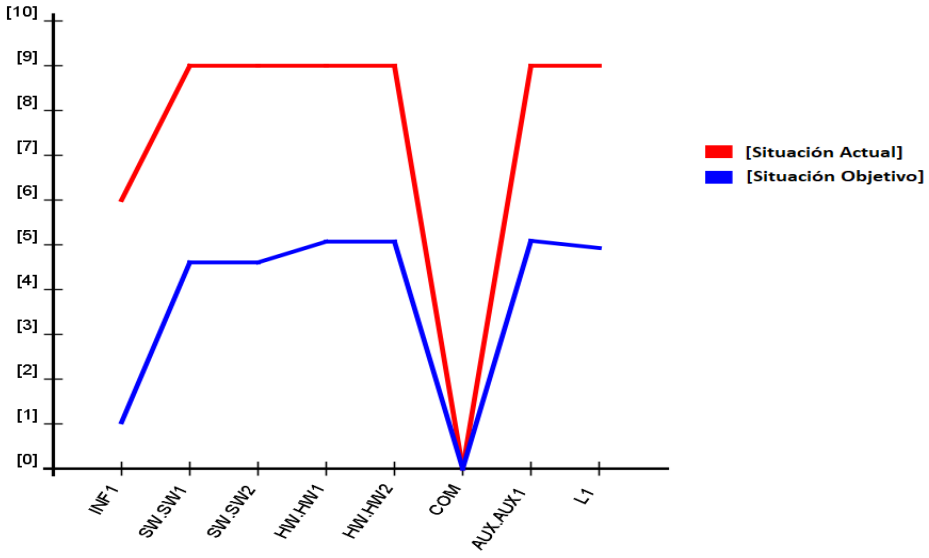
4.3. MAPA DE IMPACTO POTENCIAL VS IMPACTO RESIDUAL

Figura 12. Mapa Radial de Impacto - Situación Actual VS Situación Objetivo



Fuente: autor

Figura 13. Mapa Lineal Impacto Situación Actual VS Situación Objetivo



Fuente: autor

5. CONCLUSIONES

A partir del análisis realizado a los servidores de la Institucion de Educacion Superior se evidencia que los servidores se encuentran expuestos a una gran cantidad de riesgos (los cuales se evidencian previamente) debido a todas las amenazas tangibles e intangibles que están presentes, paralelamente a la evolucion de las teconologias de la informacion. De éste analisis, se concluye lo siguiente:

- Existen herramientas y metodologias que permiten identificar, prevenir y en caso de materializarse, mitigar todas los riesgos encontrados. Para el caso de estudio, se utilizó la metodologia Magerit, la cual propuso un esquema de estudio, donde se evidenció el estado actual de los activos, frente a riesgos informaticos y con los controles formulados ls metodologia brindó un estado objetivo e ideal para los activos de la Institucion.

- Se mostró a la Institución el estado actual de los niveles de riesgos de los servidores y el estado objetivo e ideal con el fin de que a partir de la verificacion de las estrategias y controles aplicados, la Institución analice como disminuyen los niveles de riesgo e impacto de estos activos frente a las amenazas detectadas por medio de graficas descriptivas y mapas de calor.

- Se identificó los vectores, amenazas y riesgos potenciales que pueden afectar la operación continua de la institución, dando a conocer de cada uno la probabilidad de ocurrencia, la degradación de la vida util de los activos y el impacto potencial sobre los equipos e información propios de la institución.

- Se generó una serie de estrategias que acopladas con las salvaguradas permiten mitigar el riesgo y preparar la institucion para una eventual presentación de un incidente. Así mismo estas estrategias muestran diferentes herramientas que desplegadas no solo mitigan los riesgos, sino que permiten exponer monitoreo e informes de los activos en tiempo real.

- Se entregó una guía a la institución dando a conocer todas las amenazas, vectores de ataque, riesgos encontrados y una serie de estrategias que paralelamente con los mapas de calor muestran las variaciones de los niveles de riesgo e impacto, antes y después de aplicar las salvaguardas propuestas.

6. RECOMENDACIONES

A partir del análisis y evaluación de riesgos sobre los activos presentados, se presentan las siguientes recomendaciones, con el fin de que todas se tengan en cuenta en la Universidad:

- Se sugiere realizar el análisis de las amenazas y riesgos presentados verificando que los controles formulados se estén aplicando o se apliquen en la Institución para tener un mayor control sobre los activos y las amenazas asociadas a éstos.
- Se recomienda tener en cuenta que los riesgos y los controles pueden variar de acuerdo a posibles escenarios como por ejemplo cambios sobre la infraestructura tecnológica o la implementación de nuevos proyectos lo que conlleva realizar o actualizar el análisis de riesgos realizado con el fin de mantener los niveles de seguridad independientemente los cambios en la Institución.
- Se propone crear o si se tiene, actualizar, un sistema de gestión de incidencias el cual permita gestionar cualquier amenaza o vulnerabilidad materializada y también permita recopilar las incidencias que tengan los usuarios con el fin de detectar y controlar nuevas amenazas.
- Se sugiere actualizar o realizar una política de revisión periódica de los sistemas de incidencias y al sistema de seguridad de la información con el fin de que se encuentren funcionando correctamente.
- Se recomienda incluir en los procesos de seguridad informática y la seguridad de la información de la Universidad Católica de Colombia el análisis de riesgos realizado para aumentar y mantener controlados los niveles en la seguridad de la información.

BIBLIOGRAFÍA

ÁLVAREZ MARAÑÓN, G., & PÉREZ GARCÍA, P. P. Seguridad informática para empresas y particulares. 2004. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://site.ebrary.com/ lib/unadsp/doc Detail.action? docI D=10498

BASTIDAS, E., & Guillermo, C. (2017). Identificación de vulnerabilidades de los servicios tecnológicos de la unión de cooperativas de ahorro y crédito del norte aplicando la práctica de Pentesting. . [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://repositorio.utn.edu.ec/handle/ 1234567 89/7396

COMISION DE REGULACION DE TELECOMUNICACIONES. Resolución 1732 de 17 de sep. De 2007. Colombia: Diario Oficial No. 46.756. 2007. 58 p.

CONSEJO SUPERIOR DE LA JUDICATURA. Acuerdo nº PSAA06-3334 de 2 de marzo de 2006. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://normograma.info>docs>pdf> acuerdo__csjudicatura_3334_2006

CORTE CONSTITUCIONAL. Ley 1266 de 31 de diciembre de 2008. Colombia: Diario Oficial nº 47.219. 2008. 9 p.

COSTAS SANTOS, J. Seguridad y alta disponibilidad. 2014 [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://site.ebrary.com/lib/unadsp/docDetail.action?docID=11046042

DÍAZ, F. J., HARARI, V., & VENOSA, P. Auditoría de seguridad de organizaciones, fortalezas y debilidades de la norma ISO 17799. Presentado en V Workshop de Investigadores en Ciencias de la Computación. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://hdl.handle. net/109 15/21394

DIRECCIÓN NACIONAL DEL DERECHO DE AUTOR. Decreto 1360, de 23 de junio de 1989. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https://propiedadintelectual.unal.edu.co. recursos>docs>normatividad

ESCRIVÁ GASCÓ, G., ROMERO SERRANO, R. M., & RAMADA, D. J. Seguridad informática. 2013. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://site.ebrary.com/lib/unadsp/docDetail. action?docID=10820963

FROZEN Y ICEBERG. Probabilidad de ocurrencia. [En línea], [consultado el 23 de septiembre de 2019]. Disponible en: https:// www.academia.edu › Iceberg_catalogue

FUNCION PÚBLICA. Ley 962 de julio 8 de 2005. Colombia: Diario Oficial 45963, 2005. 17 p,

GALINDO, G., & MAURICIO, D. Desarrollo del sistema de gestión de seguridad de la información (sgsi) alineado con el estándar iso 27001 y sus requisitos básicos en la aplicación del ciclo phva. 11. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: https://idus.us.es/xmlui/handle/11441/45643.

GOMEZ LOPEZ & GÒMEZ LÓPEZ. Seguridad informática. 2014. Bogotá: Editorial Rama. 108 p.

JIMÉNEZ, L. de, & Elizabeth, R. (2017). Pruebas de penetración en aplicaciones web usando hackeo ético. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://www.redicces.org.sv:80/ jspui/handle/10972/3018

LEGISLACIÓN INFORMÁTICA DE COLOMBIA. Ley de Protección de datos de 1988. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: Informática Jurídica website: http://www.informatica-juridica.com/legislacion/colombia/

LEGISLACION INFORMATICA DE COLOMBIA. Proyecto de ley estatutaria No. 1266. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Decreto 1900 de 1990. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.informatica-juridica.com.>legislacion-informatica

_____. Decreto 2150 de 1995. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.informatica-juridica.com.>legislacion-informatica

_____. Ley 527 de agosto 18 de 1999. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.informatica-juridica.com.>legislacion-informatica

_____. Resolución 7652/2000, de 22 de septiembre [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Ley 35 de 2001. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Ley 679 de 3 de agosto de 2001. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Decreto 55 de febrero 15 de 2002 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Resolución 600/2002 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Resolución 20 de 2003 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/colombia/

_____. Ley 890 de 7 de julio de 2004. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/ colombia/

_____. Ley 892 de 7 de julio 2004. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: website: http://www.informatica-juridica. com/ legislacion/ colombia/

LUJÁN MORA, S. Programación de aplicaciones web: historia, principios básicos y clientes web. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://rua.ua.es/dspace/handle/10045/16995

MAGERIT, Pilar. Metodología de análisis y gestión de riesgos de los sistemas de información. V. 3 [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https:// administracióneléctronica. gob.es> pae.home>

_____. Herramientas para el análisis de riesgos. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: https:// www.ccn-cert.cni.es › soluciones-seguridad › ear-pilar

MAIWALD, E., & MIGUEL, E. A. Fundamentos de seguridad de redes. México: McGraw-Hill, 2005.

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Resolución 1271 de 24 de junio de 2004. En línea], [consultado el 7 de octubre de 2019]. Disponible en: www.mincit.gov.co.Resolucion-1271-del-24-de junio-de-2005.

PINZÓN, G., & ALFONSO, H. Pentesting al proyecto web «Quadodo Login Script» desarrollado y soportado en lenguaje PHP versión 5.5.0. 2017. [En línea], [consultado el 7 de octubre de 2019]. Disponible en: http://repository.unad. edu.co/handle/10596/13378

PONCE, S., & PATRICIO, E. (2018). Análisis de los ataques a aplicaciones web SQL Injection y Cross Site Scripting y sus medidas de precaución y defensa. [En

línea], [consultado el 7 de octubre de 2019]. Disponible en: http://repositorio. utn.edu.ec/handle/123456789/7803

RAYA CABRERA & RAYA GONZALEZ. Riesgo Informático. Bogotá: Grupo Editorial Norma, 2014. 356 p.

RAZO, C. M. Auditoría en sistemas computacionales. México: Pearson Educación, 2002. 970 p.

RED NACIONAL DE FOMENTO AL TELETRABAJO. Ley 1221 de julio 16 de 2008. Diario Oficial No. 47052. 2007. 58 p.

REVISTA SEMANA. Así está Colombia en el ranking de ciberseguridad mundial. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: website: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

ROYER. 2004. Estudio comparativo entre las metodologías cramm y magerit para la gestión de riesgo de ti en las mpymes. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: revistas.uazuay.edu.ec>index-php.

RUIZ PALMERO, J., & SÁNCHEZ RODRÍGUEZ, J. El impacto del proyecto de centros TIC desde la experiencia vivida por el alumnado. 2007. [En línea], [consultado el 2 de marzo de 2019]. Disponible en: https://idus.us.es/ xmlui/ handle/11441/45643.

SAUCEDO, A. L. H., & MIRANDA, J. M. (2016). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web. 4(1). 2016 [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://revistas cientificas.udg.mx/index.php/REC/article/view/5208

SOLARTE, F. N. S., ROSERO, E. R. E., & BENAVIDES, M. del C. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5). [En línea], [consultado el 2 de marzo de 2019]. Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456